

Early Learning Coalition of Broward County, Inc.

Governance Meeting Agenda

September 24, 2026, at 11:00 AM

Zoom Meeting

Meeting ID: 821 1210 3653

Passcode: 476544

<https://us06web.zoom.us/j/82112103653?pwd=gxVtTXb44JUgD7Zxlu3gRj57mMnkMt.1>

Members are reminded of conflict-of-interest provisions. In declaring a conflict, please refrain from voting or discussing and declare the following information: 1) Your name and position on the Board, 2) The nature of the conflict, and 3) Who will gain or lose as a result of the conflict. Please also fill out form 8B prior to the meeting.

PAGE			
1.	Call to Order		Dawn Liberta, Governance Committee Chair
2.	Roll Call		Melody Martinez, Board Liaison
3.	Consent Agenda 1. Approve June 15, 2026, meeting minutes	2	Dawn Liberta, Governance Committee Chair
4.	Regular Business 1. GOV271RB1- Adopt Required 403B Retirement Plan Document Restatement 2. GOV271RB2- Authorize Retirement Plan Governance Framework Procurement Plan 3. GOV271RB3- Approve FY 27 Strategic Plan updates for Year 5 4. GOV271RB4- Approve Revised Data Security Policy #IT-POL-001 5. GOV271RB5- Approve Revised AI Policy #IT-POL-002 6. GOV271RB6- Approve Remote and Hybrid Work Policy #HR-POL-001	5 7 13 18 74 87	Dawn Liberta, Governance Committee Chair Christine Klima, CAO Hubert Cesar, COO
5.	Old Business New Business Matters from the Committee Public Comment		
6.	Next ELC Governance Meeting: TBD (December)		
7.	Adjourn		

Please Note: Agenda is subject to revisions and additions at the discretion of the Chair of the Coalition. Notification will be sent of any such revisions or additions. **Members of the Public:** Please sign up at the entry desk for public comments to be made on any particular agenda items no later than five minutes after the Coalition meeting has been called to order.

“As per [§286.0105, Fla. Stat.](#) Any person who decides to appeal any decision of the Board with respect to any matter considered at this meeting will need a record of the proceedings and for such purpose, may need to ensure that a verbatim record of the proceedings is made which record includes testimony and evidence upon which the appeal is to be based.”

Early Learning Coalition of Broward County, Inc.
Governance Meeting Minutes
June 15, 2026, at 10:00 AM
Zoom Meeting

Members in Attendance	Chair Dawn Liberta; Michael Asseff; Kirk Englehardt; Carol Hylton; Renee Podolsky; Amoy Reid
Members Absent (Excused)	Laurie Sallarulo
Members Absent (Unexcused)	
Staff in Attendance	Renee Jaffe, CEO; Christine Klima, CAO; Hubert Cesar, COO; Melody Martinez, Board Liaison & Executive Assistant; Lizbeth DelVecchio, Manager, Exec. Office & Board Operations; Amy Moore, VP of Family Services & Com. Engagement; Allison Metsch, VP of Education; Ancel Pratt, Sr. Dir. of Communications; Magdalena Laino, Quality Assurance Manager; Sandra Paul, Sr. Dir. of Provider Reimbursement; Stephanie Landreville, Controller
Others in Attendance	Julie Klahr, Legal Counsel

Item	Action/Discussion
Welcome & Call to Order	Chair Dawn Liberta called the meeting to order at 10:02 AM. The roll was called, and a quorum was established.
Consent Agenda 1. Approve January 29, 2026, meeting minutes	A Motion was made by Carol Hylton and Seconded by Amoy Reid to approve the Consent Agenda. The motion was Unanimously Approved. Motion Passed.
Regular Committee 1. GOV264RB1 – Approve Employee Benefits Policies for Plan Year 2026-2027	<u>Employee Health Benefit Policy Renewals (FY 2026-2027)</u> Christine Klima, CAO, reported on the proposed employee health benefit insurance renewals and coverage levels for the 2026–2027 plan year. She outlined staff’s recommendation to continue current coverage with Florida Blue for medical and Lincoln Financial for ancillary benefits, citing cost stability, employee feedback, and overall program value. The total estimated premium is \$4,683,433, with the majority employer-funded. Renee Jaffe, CEO, noted that approximately 75% of employees who responded to the survey were satisfied or very satisfied with the current carrier, and that staff feedback was a key factor in the decision to remain with Florida Blue. Carol Hylton inquired about the impact of Broward Health and Memorial Healthcare System being out-of-network. Renee Jaffe explained that employees have access to other in-network providers throughout Broward County, and those most impacted have transitioned to in-network physicians. She added that Florida Blue provided support in identifying alternative care options. Renee Podolsky further noted that other hospitals, including Holy Cross and HCA facilities, remain in-network. A Motion was made by Amoy Reid and Seconded by Renee Podolsky to Approve Proposed FY27 Employee Health Benefit Insurance Policy Renewals and Coverage Levels as Presented

2. GOV264RB2- Proposed update to ELC time off policy	<u>Update to Personal Time Off Policy</u> Christine Klima, CAO, reported on the proposed update to the Personal Time Off (PTO) policy, recommending an increase in PTO from three (3) days to five (5) days annually for eligible full-time employees, effective July 1, 2026. She noted the change is intended to enhance overall compensation and support employee recruitment, retention, and well-being A Motion was made by Kirk Englehardt and Seconded by Carol Hylton to Approve Update to Personal Time Off Policy for Eligible Staff Effective July 1, 2026. The motion was Unanimously Approved. Motion Passed.
3. GOV264RB3- Approve Retroactive Amendments 1 through 3 to ELC's 403B Retirement Plan Document	<u>Amendments to 403B Retirement Plan:</u> Christine Klima, CAO, reported on proposed amendments to the Coalition's 403B Retirement Plan to comply with an IRS Compliance Statement issued February 11, 2026. She explained that the amendments are part of corrective actions to address historical compliance issues and align plan documents with prior operational practices. The changes are retroactive and required to maintain compliance with IRS requirements. The following Motion was presented: Adopt retroactive amendment numbers 1, 2, and 3 to the Coalition's 403B Retirement Plan Document in Accordance with a Compliance Statement Issued by the IRS on February 11, 2026: Amendment 1 A Motion was made by Carol Hylton and Seconded by Renee Podolsky to: 1. Amend Broward School Readiness Coalition Retirement Plan Document dated August 13, 2002, Section 6.01C as presented for the period September 1, 2002, through December 31, 2019 Amendment 2 A Motion was made by Renee Podolsky and Seconded by Carol Hylton to: 2. Amend Broward School Readiness Coalition Retirement Plan Document dated August 13, 2002, Section 6.02 as presented for the period January 1, 2014, through September 30, 2017 Amendment 3 A Motion was made by Amoy Reid and Seconded by Kirk Englehardt to: 3. Further amend Broward School Readiness Coalition Retirement Plan Document dated August 13, 2002, Section 6.02, as presented for the period October 1, 2017, through December 31, 2019
4. GOV264RB4- Approve Risk Management Policies for Fiscal Year 2026-2027	<u>Risk Management Policies (FY 2026–2027)</u> Christine Klima, CAO, reported on the proposed FY27 Risk Management Insurance Policy renewals and coverage levels, noting continued coverage with existing carriers and overall cost savings. A Motion was made by Carol Hylton and Seconded by Amoy Reid to Approve Proposed FY27 Risk Management Insurance Policy Renewals and Coverage Levels as Presented
Unfinished Business	None
New Business	None

Matters from the Chair	None
Public Comments	None
Next Meeting	<u>TBD</u>
Adjourn	Meeting adjourned at 10:27 AM by Carol Hylton and Seconded by Kirk Englehardt

These minutes contain the action items of the Board meeting of the Early Learning Coalition of Broward. They do not include all of the Committee's discussions or comments on each matter or issue raised during the meeting. A tape recording of the meeting is held in the Coalition office. Corrections from the Committee will be taken before approval at the next meeting.

DRAFT

ITEM/MEETING	GOV267RB1/Governance Committee
DATE:	September 24, 2026
SUBJECT:	Required 403B Retirement Plan Document Restatement
FOR ACTION:	Yes
RECOMMENDED ACTIONS:	Adopt the Cycle 2 IRS Pre-Approved 403(b) Basic Plan Document and the associated Early Learning Coalition of Broward County, Inc. 501(c)(3) Pre-Approved 403(b) Plan Adoption Agreement #08-001, effective January 1, 2026
FINANCIAL IMPACT:	None
AS RECOMMENDED BY	Staff
ELC STAFF LEAD	C. Klima

Background Information:

The Coalition sponsors a 403(b) retirement plan for eligible employees and uses a bundled retirement plan service provider that supplies the Plan's recordkeeping platform, participant administration services, and IRS pre-approved plan documents. The provider's pre-approved plan document program allows the Coalition to rely on a plan that has been reviewed and approved by the Internal Revenue Service, reducing the legal and administrative risk of maintaining a separately drafted plan document and supporting ongoing compliance with applicable tax requirements.

The proposed Cycle 2 IRS Pre-Approved 403(b) Basic Plan Document replaces the version adopted by the Coalition in 2020, which has been amended periodically to reflect legislative and regulatory changes. The new Plan Document consolidates those amendments and incorporates additional updates required under federal law, including changes resulting from the SECURE Act, CARES Act, and SECURE 2.0 Act. The Internal Revenue Service requires all 403(b) plan sponsors to update their plans to reflect these legislative changes no later than December 31, 2026. The new Plan Document satisfies that requirement and is effective retroactively to January 1, 2026.

Because the Basic Plan Document has been pre-approved by the IRS, it must be adopted as written and cannot be customized by the Coalition. The associated Early Learning Coalition of Broward County, Inc. 501(c)(3) Pre-Approved 403(b) Plan Adoption Agreement #08-001 contains the Coalition's plan-specific elections from the options available under the IRS-approved document

Current Status:

In addition to several administrative and legal updates, the new Plan Document makes available a variety of retirement plan features authorized under the SECURE Act, CARES Act, and SECURE 2.0 Act that the Coalition may consider in the future. Key features include:

- Roth employer contribution options;
- Qualified student loan matching contributions;
- Long-term part-time employee participation provisions;
- Emergency savings account (PLESA) provisions;
- Emergency personal expense distributions;
- Domestic abuse distributions;
- Qualified birth and adoption distributions; and
- Other participant flexibility provisions authorized by SECURE 2.0.

Adoption of the new Plan Document makes these features available for future consideration but does not yet implement them. The associated Adoption Agreement maintains the Coalition's current plan elections without changes. Over the coming months, staff will evaluate the potential benefits, compliance requirements, administrative impact, and costs associated with these and other available options and will bring any future recommendations for changes to the Committee for consideration. A copy of the new Plan Documents with tracked changes is attached for reference, along with the draft Adoption Agreement with our Coalition-specific elections marked.

Recommended Action from Staff:

Adopt the Cycle 2 IRS Pre-Approved 403(b) Basic Plan Document and the associated Early Learning Coalition of Broward County, Inc. 501(c)(3) Pre-Approved 403(b) Plan Adoption Agreement #08-001, effective January 1, 2026

Supporting Documents:

- Draft Cycle 2 IRS Pre-Approved 403(b) Basic Plan Document with Tracked Changes (separate link)
- Draft Early Learning Coalition of Broward County, Inc. 501(c)(3) Pre-Approved 403(b) Plan Adoption Agreement #08-001. (separate link)

ITEM/MEETING	GOV267RB2/Governance Committee
DATE:	September 24, 2026
SUBJECT:	403B Retirement Plan Governance Strengthening Procurement Plan
FOR ACTION:	Yes
RECOMMENDED ACTIONS:	Authorize staff to issue Requests for Proposals (RFPs) for: • A Section 3(21) Fiduciary Advisor to serve as an independent fiduciary advisor to the Board regarding the Coalition's 403(b) Retirement Plan; and • A bundled retirement plan service vendor\ to provide recordkeeping, administration, participant services, investment platform support, and related retirement plan services.
FINANCIAL IMPACT:	TBD
AS RECOMMENDED BY	Staff
ELC STAFF LEAD	C. Klima

Background Information:

The Coalition sponsors a 403(b)-retirement plan for eligible employees and is responsible for prudent oversight of the Plan and its service providers.

As Committee members are aware, the Coalition Plan recently completed a Voluntary Correction Program (VCP) process with the Internal Revenue Service that spanned nearly a decade. In issuing its Statement of Compliance, the Internal Revenue Service reinforced the importance of strong governance, documented procedures, compliance monitoring, and specialized retirement plan expertise.

The Coalition's 403(b) Plan is approaching approximately \$10 million in assets and has become increasingly complex from a fiduciary, compliance, and administrative perspective. In addition, the Coalition's current retirement plan service provider has undergone three corporate mergers during its tenure with the Plan. Each merger resulted in changes in personnel, service teams, platform functionality, and service delivery practices that required adjustments by staff and participants and created operational disruption over time. Staff recommends evaluating available alternatives to ensure the Plan is supported by a provider with the stability, capabilities, service model, and governance resources needed to meet the Coalition's long-term needs.

The Coalition's independent auditors have also strongly encouraged the Coalition to evaluate alternatives to its current retirement plan structure and service arrangements and to complete a transition to a new retirement plan provider effective January 1, 2027. While the timeline is ambitious, staff believe it provides sufficient opportunity to complete a competitive procurement process, establish an enhanced governance framework, and complete the administrative and compliance activities necessary to support a successful transition.

Current Status:

A. Proposed Retirement Plan Governance Framework

Staff recommends a phased approach to strengthen the Coalition's retirement plan governance framework and transition to a new retirement plan platform effective January 1, 2027.

Under the proposed governance structure:

- The Board will continue to serve as the Plan fiduciary and retain ultimate decision-making authority.
- Staff will oversee Plan operations, service-provider relationships, compliance activities, procurement efforts, and implementation of Board directives.
- A Section 3(21) Fiduciary Advisor will serve as a co-fiduciary advisor to the Board, providing investment oversight, fee monitoring, fiduciary guidance, governance support, service-provider evaluation, and fiduciary education.
- A bundled service provider will perform the day-to-day recordkeeping, administration, participant services, and operational functions necessary to support the Plan.

The proposed framework will:

- Enhance fiduciary oversight;
- Strengthen compliance monitoring;
- Improve fee transparency;
- Provide independent retirement plan expertise; and
- Establish clear accountability among the Board, staff, advisors, and service providers.

A detailed summary of responsibilities is provided in Attachment A: Retirement Plan Governance Framework Roles and Responsibilities Matrix.

B. Phase 1 (October-November 2026): Procure a Section 3(21) Fiduciary Advisor

Procure an independent Section 3(21) Fiduciary Advisor to provide the Board with independent fiduciary expertise throughout the provider selection process.

The advisor will:

- Serve as a fiduciary co-advisor to the Board;
- Assist with selecting a bundled service provider and recordkeeper;
- Benchmark and monitor fees;
- Monitor service-provider performance and compliance;
- Establish and convene a Plan Governance Committee and facilitate periodic governance reviews;
- Review investment options and investment performance;
- Support development and periodic review of governance and investment policies;
- Provide fiduciary education to Board members and staff; and
- Support compliance monitoring, risk management, and fiduciary best practices.

The advisor will educate and advise the Board on retirement plan governance, fiduciary responsibilities, investment oversight, and industry best practices, but will not provide legal or tax advice.

C. Phase 2 (November-December 2026): Procure a Retirement Plan Recordkeeper and Administration Platform

Following Board approval of the Section 3(21) Fiduciary Advisor, staff and the advisor will evaluate and select a bundled retirement plan administration and recordkeeping platform.

The evaluation will consider:

- Service capabilities and participant experience;
- Platform functionality and reporting;
- Fee structure and transparency;
- Fiduciary and compliance resources;
- Cybersecurity controls;
- Implementation capabilities;
- Organizational stability; and
- Overall value to participants and the Plan.

The advisor will assist with evaluation criteria, proposal review, fee benchmarking, due diligence, and provider recommendations.

D. Governance Development, Transition Preparation, and Implementation

Throughout the process, staff will work with the selected providers, ERISA counsel, and other advisors to develop the governance framework and complete activities necessary to support a January 1, 2027, transition.

Key activities include:

- Developing a Retirement Plan Governance and Operations Manual;
- Reviewing administrative procedures and internal controls;
- Reviewing participant and historical Plan records;
- Updating participant data, as necessary;
- Evaluating investment lineups and fee arrangements;
- Coordinating data conversion;
- Preparing participant communications;
- Establishing governance, monitoring, and reporting procedures; and
- Completing implementation and readiness activities.

Following implementation, staff, the Section 3(21) Fiduciary Advisor, and the bundled service provider will monitor performance, participant experience, and operational results to support a successful transition and ongoing administration of the Plan.

Recommended Action from Staff:

Authorize staff to issue Requests for Proposals (RFPs) for:

- A Section 3(21) Fiduciary Advisor to serve as an independent fiduciary advisor to the Board regarding the Coalition's 403(b) Retirement Plan; and
- A bundled retirement plan service vendor\ to provide recordkeeping, administration, participant services, investment platform support, and related retirement plan services.

Supporting Documents:

- Retirement Plan Governance Roles Matrix

Proposed Coalition 403(b) Retirement Plan Governance Framework

Roles and Responsibilities

Area	Board / Governance Committee	Staff	Section 3(21) Financial Advisor	Bundled Service Provider	ERISA Counsel
Fiduciary Oversight	Fiduciary; approves major decisions	Supports and implements Board direction	Provides independent guidance	Provides information and reporting	Provides legal advice
Provider Selection	Approves advisor and provider selection	Leads RFP and evaluation process	Assists with evaluation and recommendations	Responds to RFP	Reviews contracts
Investments & Fees	Reviews recommendations	Monitors implementation	Benchmarks fees; monitors investments	Provides platform and fee disclosures	Advises on fiduciary issues
Compliance & Risk	Receives oversight reports	Coordinates compliance activities	Assesses governance and compliance risks	Provides administrative support	Provides legal compliance guidance
Participant Services	Oversight role	Coordinates communications	Evaluates service quality	Provides education, account services, and participant support	As needed
Governance Manual	Approves framework	Develops and maintains	Assists with development	Provides operational procedures	Reviews legal sufficiency
Transition Planning	Approves major decisions	Coordinates implementation	Provides oversight and guidance	Executes conversion activities	Reviews legal requirements

Activity	Governance Committee / Board	Staff
Authorize Governance Initiative	✓	Recommends
Select Financial Advisor	✓	Evaluates and recommends
Select Bundled Provider	✓	Evaluates and recommends

Approve Governance Manual	✓	Develops and maintains
Approve Provider Transition	✓	Coordinates implementation
Ongoing Plan Oversight	Receives reports and provides direction	Monitors operations and vendors

MEETING	GOV271RB3/ Governance Committee
DATE:	September 24, 2026
SUBJECT:	Updated 5 Year Strategic Plan
FOR ACTION:	Yes
RECOMMENDED ACTION:	Accept the recommended changes to the updated 5-Year Strategic Plan
FINANCIAL IMPACT:	No
AS RECOMMENDED BY:	Staff
ELC STAFF LEAD	H. Cesar

Background Information:

Each year following the close of the fiscal year, staff complete an annual review of strategic goals, objectives, and performance measures to assess overall progress and ensure continued alignment with organizational priorities. This review process provides an opportunity to evaluate performance trends, identify areas for continued focus, and determine whether adjustments are needed to support successful achievement of the Plan's intended outcomes.

The plan was last updated at the Sep 4, 2025, Governance, and then Sep 15, 2025, Board Meeting.

Based on the Year 4 review, staff identified several opportunities to strengthen alignment between planned activities, performance measures, and strategic priorities as the Coalition moves into the final year of implementation. These refinements are intended to support continued progress toward the goals established in the Strategic Plan.

Current Status:

Following a review of the Strategic Plan at the conclusion of FY 25/26, ELC staff recommend several targeted updates for Year 5, the final year of the current Strategic Plan, to better align measures with current priorities, operating conditions, and expected outcomes. For example, the annual community outreach target was increased from 20 to 40 events, the VPK enrollment target was increased from 11,119 to 12,560 children, and several measures were moved from semi-annual to quarterly reporting to provide more timely performance monitoring. Additional refinements included updates to select performance targets and measures based on Year 4 results and implementation experience. These changes are intended to support successful implementation during the final year of the Strategic Plan. All updates recommended for FY 25/26 can be seen in the supporting documentation.

Recommended Action from Staff:

Accept the recommended changes to the updated 5-year Strategic Plan.

Supporting Documents

- Proposed Strategic Plan with marked changes
- Proposed Strategic Plan with no marked changes

5 Year Strategic Plan 2022-2027 GOALS
Revisions Year 4 to Year 5 (with Mark Ups)

Objective	Outcomes	Target	REPORTING FREQUENCY	Year 4 - Total Count or Average %	Revisions/Justification
1. Deploy a successful targeted outreach and enrollment initiative	1. ELC staff will actively attend a minimum of 20 community outreach events annually to promote its services.	20 Annually 40 Annually	Quarterly	34	Revision: Target changed from 20 Annually to 40 Annually Justification: Exceeded Goal
	2. ELC communications staff will discuss the importance of childcare/ early learning and the services ELC provides. They will place a minimum of 800 social media posts concerning the importance of childcare and early learning, and the services ELC	800 annually	Quarterly	1,239	
2. Families that are eligible to continue receiving SR services will receive them.	1. The overall retention rates for potentially SR-eligible families wi stabilize at 75%	75%	Semi-Annually	76.50%	
Objective	Outcomes	Target	REPORTING FREQUENCY	Year 4 - Total Count or Average %	Revisions/Justification
1. ELC will reach and enroll as many VPK-eligible families as possible.	1. ELC Broward will meet or exceed the State of Florida estimating conference estimates for VPK	11,119 12,560	Semi-Annually Quarterly	12,038	Revision: Target changed from 11,119 to 12,560 Reporting Frequency changed from Semi-Annually to Quarterly Justification: Updated Estimated VPK Enrollments for School Year 26/27 by the State's Estimating Conference held in August 2026
Objective	Outcomes	Target	REPORTING FREQUENCY	Year 4 - Total Count or Average %	Revisions/Justification
1. The countywide CLASS score average for CLASS assessed will increase to a 6.0	1. CLASS scores will incrementally grow year over year for the 5 year strategic plan.	6 5.6	Annually	5.56%	Revision: Target changed from 6 to 5.6 Justification: The higher the quality level, the harder to achieve additional gains
Objective	Outcomes	Target	REPORTING FREQUENCY	Year 4 - Total Count or Average %	Revisions/Justification
Objective 1: The countywide CLASS score average for VPK child care providers who are CLASS assessed will increase to a 6.0	1. CLASS scores will incrementally grow year over year for the 5 year strategic plan.	6 5.7	Annually	5.67%	Revision: Target changed from 6 to 5.7 Justification: The higher the quality level, the harder to achieve additional gains
Objective	Outcomes	Target	REPORTING FREQUENCY	Year 4 - Total Count or Average %	Revisions/Justification
1. SR and VPK children will receive support (developmental, behavioral, health, etc.) to maximize their developmental potential.	1. 65% of families with children ages 0-2 who have received a referral will follow through with their referrals to Early Steps	65% 80%	Quarterly	91.50%	Revision: Target changed from 65% to 80% Justification: Exceeded Goal, adjusted to realistic stretch goal
		75%	Quarterly	73.25%	
	3. Through funding or partnerships, four (4) additional, comprehensive support services will be added or expanded to children/families (such as but not limited to vision, hearing, dental	4	Annually	13	

2. Expand ELC Literacy efforts to increase the number of children who have access to books/libraries at home as well as increased exposure to the reading experience	1. Increase # of families with children under 5 who sign up for ELC's bookworm program to 15,000	7,500 Based on reduced- BW budgeted of \$200K Expend 95% of allocated Book Worms resources	Quarterly	6,868	Revision: Target changed from "7,500 Based on reduced BW budgeted of \$200K" to "Expend 95% of allocated Book Worms resources" Justification: with moving annual budget allocation throughout the year, it makes sense to use % of total than number as target measure.
	2. ELC will participate in at least 20 outreach literacy / learning events throughout the year, utilizing new and existing partnerships/events, as well as creating its own.	20	Quarterly	42	Revision: Outcomes replaced "outreach" with " literacy / learning" Justification: Objective related to increased lieteracy efforts
Goal 6. The ELC has strong relationships with community leaders and other stakeholders to mobilize all parts of our community to support early learning.					
Objective	Outcomes	Target	REPORTING FREQUENCY	Year 4 - Total Count or Average %	Revisions/Justification
1. Broward County leaders are aware of the importance of early learning, ELC Services, and ELC Legislative Priorities.	1. At the start of each fiscal year, ELC staff will identify which state legislators, Broward County Commissioners/County Administration, and elected municipal leaders, they need to meet with and meet with 100% of them.	90%	Semi-Annually Quarterly	100.00%	Revision: Reporting Frequency changed from Semi-Annually to Quarterly Justification: Less vague; aligned with quarterly score card reviews
2. ELC will strengthen relationships and partnerships with Community leaders and stakeholders through participation in early learning activities/events.	1. ELC will actively participate in a minimum of 30 community engagement activities/events annually to promote ELC's services.	30	Semi-Annually Quarterly	34	Revision: Reporting Frequency changed from Semi-Annually to Quarterly Justification: Less vague; aligned with quarterly score card reviews
Goal 7. ELC Broward is a healthy, efficient, and effective organization.					
Objective	Outcomes	Target	REPORTING FREQUENCY	Year 4 - Total Count or Average %	Revisions/Justification
1. The ELC promotes an inspired workplace culture by developing quantitative and qualitative approaches to attract, engage, and retain a talented workforce efficiently and effectively.	1. Following their probation period, ELC is retaining the right staff for the right positions, as evidenced by retaining 75% of new hires in one year following their 3 month probationary period.	75%	Semi-Annually	95.83%	
	2. ELC annual staff turnover will be at or below 15%	15%	Semi-Annually	5.38%	
	3. 35% of all available advancement opportunities are filled internally.	35%	Semi-Annually	37%	
	4. At least 85% of Staff respond that they are overall satisfied working at the ELC.	85%	Annually	80%	
2. Continue to optimize the use of technology and data to promote efficiencies, evaluate value, impact, and progress, and increase data security.	2. 90% of ELC data infrastructure will be stored in the cloud.	90%	Annually	80%	Revision: Objective 2.2 removed Justification: Achieved goal, no longer needed
4. Obtain dedicated funding for specific allowable & unallowable expenses.	1. ELC will have funds for items for meetings, programming, and training (NON FEDERAL, NON STATE, NON MATCH).	25000 100,000	Annually	\$38,596	Revision: Target changed from 25,000 to 100,000 Justification: Exceeded Goal
5. The ELC board is engaged, educated and works well with staff.	1. Results of the annual staff and board survey will show at least a 90% rating in all categories.	90%	Annually	92.30%	

5 Year Strategic Plan 2022-2027 GOALS
Revisions Year 4 to Year 5 (with no Mark Ups)

Objective	Outcomes	Target	REPORTING FREQUENCY	Year 4 - Total Count or Average %	Revisions
1. Deploy a successful targeted outreach and enrollment initiative	1. ELC staff will actively attend a minimum of 20 community outreach events annually to promote its services.	40 Annually	Quarterly	34	Target changed from 20 Annually to 40 Annually
	2. ELC communications staff will discuss the importance of childcare/ early learning and the services ELC provides. They will place a minimum of 800 social media posts concerning the importance of childcare and early learning, and the services ELC	800 annually	Quarterly	1,239	
2. Families that are eligible to continue receiving SR services will receive them.	1. The overall retention rates for potentially SR-eligible families will stabilize at 75%	75%	Semi-Annually	76.50%	
GOAL 2. Eligible families will be aware of and access ELC VPK services.					
Objective	Outcomes	Target	REPORTING FREQUENCY	Year 4 - Total Count or Average %	Revisions
1. ELC will reach and enroll as many VPK-eligible families as possible.	1. ELC Broward will meet or exceed the State of Florida estimating conference estimates for VPK	12,560	Quarterly	12,038	Target changed from 11,119 to 12,560 Reporting Frequency changed from Semi-Annually to Quarterly
Objective	Outcomes	Target	REPORTING FREQUENCY	Year 4 - Total Count or Average %	Revisions
1. The countywide CLASS score average for School Readiness child care providers who are CLASS assessed will increase to a 6.0	1. CLASS scores will incrementally grow year over year for the 5 year strategic plan.	5.6	Annually	5.56%	Target changed from 6 to 5.6
Objective	Outcomes	Target	REPORTING FREQUENCY	Year 4 - Total Count or Average %	Revisions
Objective 1: The countywide CLASS score average for VPK child care providers who are CLASS assessed will increase to a 6.0	1. CLASS scores will incrementally grow year over year for the 5 year strategic plan.	5.7	Annually	5.67%	Target changed from 6 to 5.7
Objective	Outcomes	Target	REPORTING FREQUENCY	Year 4 - Total Count or Average %	Revisions
1. SR and VPK children will receive support (developmental, behavioral, health, etc.) to maximize their developmental potential.	1. 65% of families with children ages 0-2 who have received a referral will follow through with their referrals to Early Steps	80%	Quarterly	91.50%	Target changed from 65% to 80%
	referral will follow through with their referrals to FDLRS	75%	Quarterly	73.25%	
	3. Through funding or partnerships, four (4) additional, comprehensive support services will be added or expanded to children/families (such as but not limited to vision, hearing, dental screenings, mental health, nutrition services, and general medical)	4	Annually	13	

2. Expand ELC Literacy efforts to increase the number of children who have access to books/libraries at home as well as increased exposure to the reading experience	1. Increase # of families with children under 5 who sign up for ELC's bookworm program to 15,000	Expend 95% of allocated Book Worms resources	Quarterly	6,868	Target changed from "7,500 Based on reduced BW budgeted of \$200K" to "Expend 95% of allocated Book Worms resources"
	2. ELC will participate in at least 20 literacy / learning events throughout the year, utilizing new and existing partnerships/events, as well as creating its own.	20	Quarterly	42	Outcomes replaced "outreach" with " literacy / learning"
Goal 6. The ELC has strong relationships with community leaders and other stakeholders to mobilize all parts of our community to support early learning.					
Objective	Outcomes	Target	REPORTING FREQUENCY	Year 4 - Total Count or Average %	Revisions
1. Broward County leaders are aware of the importance of early learning, ELC Services, and ELC Legislative Priorities.	1. At the start of each fiscal year, ELC staff will identify which state legislators, Broward County Commissioners/County Administration, and elected municipal leaders, they need to meet with and meet with 100% of them.	90%	Quarterly	100.00%	Reporting Frequency changed from Semi-Annually to Quarterly
2. ELC will strengthen relationships and partnerships with Community leaders and stakeholders through participation in early learning activities/events.	1. ELC will actively participate in a minimum of 30 community engagement activities/events annually to promote ELC's.	30	Quarterly	34	Outcomes the word "services" was removed Reporting Frequency changed from Semi-Annually to Quarterly
Goal 7. ELC Broward is a healthy, efficient, and effective organization.					
Objective	Outcomes	Target	REPORTING FREQUENCY	Year 4 - Total Count or Average %	Revisions
1. The ELC promotes an inspired workplace culture by developing quantitative and qualitative approaches to attract, engage, and retain a talented workforce efficiently and effectively.	1. Following their probation period, ELC is retaining the right staff for the right positions, as evidenced by retaining 75% of new hires in one year following their 3 month probationary period.	75%	Semi-Annually	95.83%	
	2. ELC annual staff turnover will be at or below 15%	15%	Semi-Annually	5.38%	
	3. 35% of all available advancement opportunities are filled internally.	35%	Semi-Annually	37%	
	4. At least 85% of Staff respond that they are overall satisfied working at the ELC.	85%	Annually	80%	
4. Obtain dedicated funding for specific allowable & unallowable expenses.	1. ELC will have funds for items for meetings, programming, and training (NON FEDERAL, NON STATE, NON MATCH).	100,000	Annually	\$38,596	Target changed from 25,000 to 100,000
5. The ELC board is engaged, educated and works well with staff.	1. Results of the annual staff and board survey will show at least a 90% rating in all categories.	90%	Annually	92.30%	

ITEM/MEETING	GOV271RB4/ Governance Committee
DATE:	September 24, 2026
SUBJECT:	ELC 2019 Data Security and Systems Policy and Procedures
FOR ACTION:	Yes
RECOMMENDED ACTION:	Approve ELC 2026 Data Security and Systems Policy and Procedures
FINANCIAL IMPACT:	None
AS RECOMMENDED BY:	Staff
Policy #	IT-POL-001
Policy History	Gov 9.16.19 GOV201RB1 / Board 10.3.19 B202CA1
ELC STAFF LEAD	H. Cesar

Background Information:

The Coalition's Data Security and Systems Policy were last comprehensively updated in 2019. Since that time, the Coalition's technology environment has evolved significantly, including increased use of cloud-based services, remote access technologies, mobile devices, and emerging artificial intelligence (AI) tools. In addition, cybersecurity threats and industry best practices have continued to evolve, requiring organizations to strengthen controls designed to protect confidential information, personally identifiable information (PII), and Coalition information systems.

Current Status

After a thorough review of the ELC's Data Security and Systems Policy and Procedures, ELC staff propose updates to the policy to better reflect the Coalition's current technology environment and cybersecurity needs. Since the policy was last comprehensively updated in 2019, the Coalition has expanded its use of cloud-based services, remote access technologies, mobile devices, and other digital tools to support daily operations. The updated policy strengthens existing security requirements and introduces additional safeguards to protect Coalition information, systems, and technology resources.

Key updates include the addition of provisions addressing Artificial Intelligence (AI) use, cloud security, multi-factor authentication (MFA), cybersecurity risk assessments, vendor cybersecurity requirements, mobile device management, and enhanced remote access controls. Examples include requiring security reviews before AI tools are connected to Coalition systems, requiring MFA for access to certain systems and applications, establishing security expectations for vendors with access to Coalition information, and requiring Coalition-managed devices for access to confidential or sensitive information.

These revisions are intended to strengthen the Coalition's cybersecurity posture, reduce information security risks, and ensure Coalition information assets remain protected while supporting efficient and secure operations.

Recommended action from Staff:

Approve ELC 2026 Data Security and Systems Policy and Procedures

Supporting Documents

- Data Security and Systems Policy and Procedures- With Marked Changes
- Data Security and Systems Policy and Procedures- With no Marked Changes



Data Security and Systems Policy and Procedures

Early Learning Coalition of Broward County

DRAFT PENDING APPROVAL

October 3, 2019

TABLE OF CONTENTS

STATEMENT OF POLICY	3
PURPOSE.....	3
STATEMENT OF PROCEDURE.....	5
DEFINITIONS	5
APPLICATION OF FEDERAL AND FLORIDA’S DISCLOSURE AND PUBLIC RECORDS LAWS.....	8
USE OF ELC SYSTEMS.....	8
ELECTRONIC TRANSMISSION.....	10
COMPLIANCE AND MONITORING	16
USER ACCOUNT MANAGEMENT PROCEDURES	16
SECURITY MANAGEMENT/ACCESS CONTROL	17
SECURITY TRAINING AND AWARENESS.....	18
ELECTRONIC MAIL	19
DATA BACKUP	20
MEDIA DEVICES/PHYSICAL/SYSTEM/DATA SECURITY	21
ANTIVIRUS	22
MOBILE COMPUTING	22
REMOTE COMPUTING	23
USE OF INTERNET/WORLDWIDE WEB.....	24
EXHIBIT A - MEMORANDUM OF UNDERSTANDING - OEL.....	27

ELC Policy Name: **Data Security and Systems Policy and Procedure**
ELC Policy No.
Approval Date: **Pending Board Approval**

STATEMENT OF POLICY

As part of its mission, the Early Learning Coalition of Broward County, Inc. ("ELC") maintains computers, servers, cell phones, data systems and a secure network. These computing resources are intended for ELC-related purposes. For purposes of this policy and procedure, "ELC systems" shall mean all computing, data, network, platforms and web/cloud based resources or systems including, but not limited to, the use of electronic mail, internet, intranet, web pages, video communication, portable devices (i.e. cell phones, jump/USB drives, storage media, etc.), computer software, computer hardware and cloud/server based storage, messaging, databases, or repositories, whether internal or external, that are owned, leased or controlled by the ELC and/or OEL, its agent(s) or other authorized third parties contracted with the ELC, that the ELC utilizes to store, transmit, distribute, create, delete or access data, records, files, documents, materials or other information that is the property of or has been licensed to the ELC and/or the Office of Early Learning ("OEL").

ELC staff have access to one or more forms of data systems and ELC encourages the use of approved data systems and associated services and products as they make communication more efficient and effective, and because they are valuable sources of information. However, all computer systems provided by ELC for employee use are the property of ELC and their purpose is to facilitate ELC business.

This policy expresses the ELC philosophy and sets forth general principles to be applied in the use of ELC systems. The ELC expects its staff to understand that they are to use good judgment when it comes to using the ELC systems. This policy is designed to provide guidance for basic principles and premises of the use of the ELC systems for the transaction of ELC business.

All ELC staff, contracted employees, Vendors, Contractors, Subcontractors, and others doing business with the ELC are expected to comply with all provisions of this policy as well as applicable federal and Florida statutes, rules and regulations. The aforementioned parties are also expected to comply with the applicable authoritative citations with the most recent funding agreement between the ELC and the applicable governing agency for the ELC ("Grant Agreement").

PURPOSE

The purpose of the data security policy is to define, develop and document the information protocols, standards, and procedures that support the ELC goals and mission to ensure that all Personal Identifiable Information (PII), assessment, and health data of all families and children served are guaranteed to be safe and confidential and release of data is in accordance with the guidance of Office of Early Learning ("OEL").

Data security policies/protocols, standards and procedures represent the foundation for ELC information security system. The policies serve as overarching guidelines for the use, management, and implementation of information security throughout the organization.

SCOPE

The Data Security Policy is an official directive of the Chief Information Officer (“CIO”) as approved by the Board. This policy applies to all employees of the ELC, its Contractors, its Vendors, its Service Providers, and any other authorized persons or entities designate by the ELC and its respective ELC systems that are:

- Accessed and/or stored on ELC premises or on the cloud;
- Accessed using ELC or ELC funded data systems;
- Accessed using ELC or ELC funded paid access methods;
- Accessed using ELC data systems from a remote location;
- Used in a manner which identifies the individual with ELC; and/or
- Used for the transaction of ELC business, including data systems that are owned by ELC, as well as those which are owned by the user and/or any other person or entity.

Board Chair’s Signature: _____

Date Signed: _____

STATEMENT OF PROCEDURE

DEFINITIONS

1. **Board** shall have the same meaning as it does in the ELC bylaws.
2. **Artificial Intelligence (AI)** means computer systems capable of performing tasks that typically require human intelligence, including generative AI, machine learning, predictive analytics, natural language processing, and large language models.
3. **Breach** shall mean a confirmed event that compromises the confidentiality, integrity, or availability of information or data (Ch. 282.0041, F.S.)
4. **Breach of Security** shall mean any unauthorized access of data containing personal information. A breach of security is shall mean an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information ("PHI"), personally identifiable information ("PII"), Protected personally identifiable information ("PPII"), trade secrets or intellectual property. Good faith access of data containing personal information by an employee or agent of ELC does not constitute a breach, provide the information is not used for a purpose unrelated to the agreement, task or subject to further unauthorized use (Ch. 501.171, F.S.).
5. **Chair** shall have the same meaning as it does in the ELC bylaws.
6. **Client** shall mean the intended recipients of the ELC and/or Florida's Office of Early Learning ("OEL") grant related activities, services or funding, including, but not limited to the ELC Voluntary Pre-Kindergarten ("VPK") or School Readiness ("SR") programs and services such as children, parents and legal guardians.
 - 1.
7. **Cloud Service Provider** means a third-party organization that hosts, processes, transmits, or stores Coalition information using internet-based services.
8. **Confidential Information or Confidential** shall mean record systems, specific records or individually identifiable data that by law are not subject to public disclosure pursuant to applicable federal and Florida statutes, codes and other regulations. When applicable, this definition or any reiteration of it covers all documents, papers, materials computer files, letters and all other notations of records, data or other information that are designed by law or contract, whichever is applicable, as confidential, including but not limited to those items that may be considered proprietary information, intellectual property, or trade secrets belonging to the ELC, OEL or a third party. Furthermore, the term "confidential" covers the verbal conveyance of data or information that is designed by law or contract confidential.
9. **Contractor** shall mean those eligible licensed entities that contract directly with the ELC to provide School Readiness or Voluntary Pre-Kindergarten services and/or programs in accordance with Florida Statutes and provides monitoring, investigations and/or other oversight functions on behalf of the ELC to Service Providers. For purposes of this policy and procedure, the term "**Contractor**" shall have the same meaning as the term "**lead agency**" or "**sub-recipient**" in any statewide agreement(s) created by the Office of Early Learning, any other governing state agency or authority for the ELC, any applicable federal or Florida statutes, or within any contract or agreement with a third party concerning VPK or SR services.

10. **ELC** shall mean the Early Learning Coalition of Broward County, Inc. For purposes of this policy and procedure, the term “**Coalition**” shall have the same meaning as the term “**ELC**”.
11. **ELC staff** means those persons directly employed by the ELC.
12. **Member** shall have the same meaning as it does in the ELC bylaws.
13. **Multi-Factor Authentication (MFA)** means an authentication method requiring two or more verification factors before granting access to a system or application.
14. **Personally Identifiable Information (“PII”)** shall mean information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.
15. **Protected Personally Identifiable Information (“PII”)** shall mean information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
16. **Public Records** shall mean any hard copy or electronic copies of records made or received by any public agency in the course of its official business. Records such as policies, meeting minutes, files, program results, computer records, emails, text messages and social media accounts are all available for inspection unless specifically exempted in state statute.
17. **Secure File Transfer Protocol (“SFTP”)** shall mean a secure method of transferring files between two remote systems.
18. **Security Incident** means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology security policies, acceptable use policies, or standard security practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing a specific incident is about to occur. A breach includes a confirmed event that compromises the confidentiality, integrity or availability of information or data. (Ch. 282.0041 F.S.).
19. **Service Providers** shall mean an eligible public school, private faith-based, licensed or license-exempt child care entity that has provider agreement with the ELC and/or a Contractor to provide Voluntary Pre-Kindergarten (“VPK”) or School Readiness (“SR”) program services directly to children in Broward County in accordance with Florida Statutes. For purposes of this policy and procedure, the term “**Service Provider**” shall have the same meaning as the term “**Provider**” in any statewide agreement(s) for VPK and SR created by the Office of Early Learning (“OEL”), any other governing state agency for the ELC, any applicable federal or Florida statutes, or within any contract or agreement with a third party concerning VPK or SR services.
20. **Subcontractor** shall mean those persons or entities that have a contract with the ELC or a Contractor and are retained to perform either a portion or all of the SR and/or VPK program related services on behalf of the Contractor or ELC under those original contracts. For purposes of this definition, “SR and/or VPK program related work” shall mean services that would not fall under the definition of a “**Vendor**” such as instructional, client engagement, monitoring, and reporting. This definition shall also exclude those person or entities that deliver or perform professional services. For purposes of this definition, “professional services” shall mean accounting, finance, audit, legal or licensed healthcare related services.

21. Vendor shall mean a dealer, distributor, merchant or seller who provides goods and services within business operations; provides similar goods or services to many different purchasers; operates in a competitive environment; provides goods or services that are ancillary to the operation of the federal program; and is not subject to compliance requirements of the federal program. For purposes of this policy and procedure, the term **“Consultant”** shall have the same meaning as the term **“Vendor”**.

APPLICATION OF FEDERAL AND FLORIDA'S DISCLOSURE AND PUBLIC RECORDS LAWS

This policy shall be subject to those applicable federal and Florida statutes, codes and regulations governing access, disclosure, distribution, alteration, retention, destruction and maintenance of public records, which would include, but not be limited to Florida's public records statute, Chapter 119. Records requests shall be done and this policy and procedure shall be subject to the ELC's Public Records Policy and Procedure. In the event there is an unallowable conflict between the ELC's Public Records Policy and Procedure and this policy and procedure, the ELC's Public Records Policy and Procedure shall control.

Electronic mail created or received by ELC staff or other authorized persons or entities as designated by the ELC in connection with official business, which perpetuates, communicates or formalizes knowledge, is subject to the public records law and is open for inspection unless specifically exempt by law or ordered by a court of law not to be disclosed by the ELC. If your electronic mail falls within the definition of a public record, you may not delete it except as provided in the ELC's records retention schedule as set forth in the ELC's Records Management Policy and Procedure. All ELC-issued cellular phones are subject to public records request per Florida Statutes Chapter 119.

USE OF ELC SYSTEMS

The ELC systems may not be used for knowingly transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature, or which are derogatory to any individual or group, or which are obscene, pornographic, suggestive or inappropriate communications, or are of a defamatory or threatening or offensive nature, or for "chain letters" or for any other purpose which is illegal or against ELC policy or contrary to the interest of ELC by ELC staff, its volunteers, its interns, its contracted third parties, or its Board Members.

The ELC systems are primarily for ELC business use. Limited, occasional or incidental use of the ELC systems for personal, non-business purposes is understandable, as is the case with personal phone calls. Such limited, occasional, or incidental use of ELC systems is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other ELC responsibilities, and is otherwise in compliance with this policy and procedure. However, subject policies set forth herein, the ELC Employee Handbook and as otherwise required by law, ELC staff need to demonstrate a sense of responsibility and may not abuse the privilege.

To safeguard data and confidential information, ELC prohibits the use of personal data storage devices on the network in order to ensure conformity and that every employee is only using an ELC approved secure-encrypted storage media or equipment (e.g. flash drives, thumb drives, etc.). ELC staff or other authorized persons or entities as designated by the ELC are not allowed to use personal computers in order to access mission critical servers/files systems, databases or other platforms, but may be given secure access to the Internet via a secured guest Wi-Fi network, which does not allow users access to ELC internal network.

Electronic information created and/or communicated by an employee that is not saved or backed-up on the ELC's server or any third -party database or cloud system utilized by the ELC, will not generally be monitored by ELC. However, the following conditions should be noted:

1. The ELC reserves the right to monitor usage patterns for all of the ELC systems.

2. The ELC also reserves the right, in its discretion, to review, monitor, audit, intercept, access, disable and/or disclose any employee's electronic files and messages and usage and/or the hard drive, portable devices, software, hardware or any other computing resource of any ELC employee for any lawful purpose including, but not limited to, ensuring that ELC resources are being used in compliance with applicable federal and Florida laws as well as in accordance with the ELC policies and procedures.
3. ELC staff or other authorized persons as designated by the ELC should not assume that electronic communication or data stored on in accordance with this policy and procedure are totally private and confidential and should take proper steps to transmit highly sensitive or personal information in accordance with this policy and procedure and applicable law. ELC staff should not assume that ELC systems are their personal property.
4. ELC staff or other authorized persons as designated by the ELC must respect the confidentiality of other people's electronic communications and may not attempt to "hack" into other systems or other people's logins, or "crack" passwords, or breach computer or network security measures or otherwise access the electronic communications in an unauthorized or unapproved manner. ELC staff or other authorized persons as designated by the ELC may not monitor electronic files or communications of other ELC staff or third parties except under the explicit direction of the Chief Information Officer or Chief Executive Officer of the ELC.
5. The ELC reserves the right to remove ELC system privileges from an employee or other authorized persons as designated by the ELC.
6. The ELC systems are not to be used for personal commercial purposes or for personal, financial or other gain.
7. No employee or other authorized persons as designated by the ELC will knowingly create access to ELC systems in such a way to bypass ELC security systems.
8. No employee or other authorized persons will use ELC systems for illegal activities.
9. All ELC staff and other authorized persons will do their best to ensure all software or data is free of any viruses, malware, trojans or other harmful programs before it is installed or loaded on the ELC data network. Any detection of any virus malware, trojans or other harmful programs must be reported immediately to the ELC's Information Technology ("IT") Department. ELC staff will be trained on a regular basis to make they are aware of data security threats.
10. Violation of this policy and/or violations of applicable laws, statutes and ordinances may result in loss or limitations on use of information technology resources related to the ELC systems as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.
11. Contractors and Vendors must sign a non-disclosure agreement protecting any confidential data to which the Contractor or Vendor requires access. A Contractor or Vendor shall ensure that the requirement to comply fully with this policy and procedure is included any agreement or contract with any Subcontractor if said Subcontractor is utilized to perform or deliver, whether in whole or in part, any ELC-related service or work done by the Contractor or Vendor. The Contractor or Vendor shall be responsible and shall be held liable for the violation of this policy and procedure by any Subcontractor utilized to perform or deliver, whether in whole or in part, any ELC-related service or work done by the Contractor or Vendor. Persons or entities authorized to confidential data as described in the policy and procedure will be required to sign a non-disclosure agreement protecting any confidential data to which the person or entity may requires access.

ARTIFICIAL INTELLIGENCE (AI) SYSTEMS

The use of Artificial Intelligence (AI), Generative AI, Machine Learning, and Large Language Model technologies must comply with the Coalition's Artificial Intelligence Acceptable Use Policy.

Users shall not enter confidential information, personally identifiable information (PII), protected health information (PHI), personnel information, provider information, financial information, or other non-public Coalition information into publicly accessible AI tools unless specifically approved by the Chief Information Officer or Information Security Manager.

AI systems connecting to Coalition data repositories, email systems, cloud environments, or business applications shall undergo a security review before implementation.

AI-generated content must be reviewed by an authorized individual before use in official Coalition operations, communications, compliance activities, or decision-making.

ELECTRONIC TRANSMISSION

Transmission Procedures

The ELC and its Contractors and its Vendors as well as any other authorized person as designated by the ELC must safeguard private and confidential data such as names, addresses, social security numbers, and federal employment numbers. Unencrypted transfer of private and confidential information by e-mail or mobile devices (flash drives, thumb drives, cell phones or laptops) is prohibited. This prohibition applies to submissions to the Office of Early Learning ("OEL"), Department of Education ("DOE"), as well as transmissions among contractors, vendors and sub-recipients. All transmission of confidential data must be secured. The ELC's IT Department strongly encourages staff and any other authorized person as designated by the ELC to transmit confidential data via OEL's SharePoint site, Secure File Transfer Protocol ("SFTP") site or via any third-party cloud system utilized by the ELC which would include but not be limited to Sharefile. The ELC currently complies with requirements for restrictions on access to sensitive or confidential data as described in OEL's IT Policy and Program Guidance.

Examples of secure transfer of confidential data, records and files include but are limited to the following:

- Encryption of a file with a program.
- The use of last names plus the last four digits of social security numbers.
- Ensure that sensitive paperwork is secured and not in view of unauthorized persons
- Transmit data behind a firewall.
- Transmit data via SFTP
- Transmit via any third-party cloud system utilized by the ELC which would include but not be limited to Sharefile

The following definitions and information can be found in the applicable OEL program guidance regarding records confidentiality:

Acceptable Use of Information Resources

Individuals using information resources or data belonging to a governmental or quasi-governmental entity or agency shall act in a legal, responsible, and secure manner, with respect for the rights of others.

Information Resources Classification

All information resources (including data and systems) shall be identified, categorized and protected according to their level of confidentiality. All files should be stored and filed appropriately on the ELC server (whether it is a physical or web/cloud-based server).

Security Training and Awareness

The ELC information technology and security policies, procedures, and protocols shall be communicated to all ELC staff or other authorized persons as designated by the ELC, and shall be available for reference. Any changes to those information technology and security policies, procedures, and protocols will be discussed at ELC staff meetings.

Incident Reporting

ELC staff, Contractor, Vendors, Service Providers, Subcontractors and other authorized persons as designated by the ELC are required to report suspected security incidents, unauthorized disclosures, or security breaches in accordance with the ELC Incident Reporting Policy and Procedure. Incident reports should be reported and forwarded to the ELC's IT Department immediately. Within 24 hours of the incident, the ELC shall provide written notification to the Office of Inspector General and the Information Security Manager.

Written notification to OEL must identify the following:

1. The nature of the unauthorized use or disclosure
2. The confidential information used or disclosed
3. Who made the unauthorized use or received the unauthorized disclosure
4. What the ELC has done or shall do to mitigate any harmful impact of the unauthorized use or disclosure and;
5. What corrective action the ELC has taken or shall take to prevent similar future unauthorized use or disclosure incidents.
6. Provide any additional information as reasonably requested by OEL.

See Incident Reporting Policy for further information.

Incident Response

The ELC shall be able to respond to computer security-related incidents in a manner that protects its own information and helps to protect the information of others that might be affected by the incident.

Incident response and reporting requirements can be found in Breach of Security/Confidentiality section of the OEL Grant Agreement. In the event there is an unallowable conflict between the Grant Agreement and the ELC's Incident Reporting Policy and Procedure, the Grant Agreement shall prevail.

Security System Plans

The ELC's computer system shall contain a firewall which shall monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

Monitoring the Adequacy of System Performance and Hardware

The ELC shall periodically monitor the following:

- (1) appropriateness of access privileges assigned to users of certain systems and hardware;
- (2) periodically reviewing the appropriateness of access privileges assigned to users of certain systems;
- (3) performance of system hardware and capacity-related issues; and
- (4) ensuring appropriate backup procedures and disaster recovery plans are in place.

Contingency Planning

Alternate modes of operation exist to ensure continuity of critical services in the event of a natural disaster, fire, act of terror, or other catastrophic event as outlined in the ELC Continuing Offsite Operations Plan ("COOP").

Access Control

Access to the ELC's systems shall be limited to those persons that need such access to perform their job or contractual duties. Procedures and protocols are to be in place to address and document the tasks that activate access to any production systems for ELC staff, its agents, its Contractors, its Vendors or other authorized persons and to deactivate/remove access to all production systems for outgoing or transferring ELC staff, its agents, its Contractors, its Vendors or other authorized persons as designated by the ELC that are in compliance with OEL's IT policy regarding personnel security. These include, but are not limited to, the following:

- Documentation for managing access criteria for information resources.
- The return of any office information resources (property or data).
- Procedures for unfriendly termination that include the prompt removal of system access.
- Audit trails shall be created and maintained to provide accountability for all access to confidential and exempt information and products.
- Audit trails for all changes to automated security or access. Examples include removal of access privileges, computer accounts and authentication tokens.

The ELC complies with requirements for deleting operational data from disposed equipment described in OEL's IT Security Policy.

Identification and Authentication

Access to ELC systems shall be granted to identified and authenticated users only.

Antivirus

This policy is in place so that the ELC, its agents, its Contractor, its Vendors or other authorized persons as designated by the ELC may verify that all computer systems are protected with antivirus and anti-malware software and that techniques are employed for avoiding viruses, malwares and other malicious programs to ELC systems.

Physical and Environmental Security

Automated information systems and facilities require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of ELC staff. Computer systems, facilities, confidential records, personally identifiable information ("PII"), protected personally identifiable information ("PPII") and disk storage areas shall be protected from theft, alteration, destruction, damage (i.e. fire, dust, misuse, water, etc.), power loss and other contaminants and unauthorized disruption of operation.

Change Control

All security changes made to any ELC systems shall be made in a controlled and coordinated fashion to preserve the confidentiality, integrity and availability of the system. No change to the ELC systems shall be made without the approval of the Chief Information Officer and the Chief Executive Officer.

Backup and Recovery

Recoverable backups shall be maintained for all critical systems at the ELC or by its contracted third party. Backups of critical information resources must be performed, tested and appropriately managed. Backups will be performed according to the following schedule:

- a. All critical data and system configurations must be backed up on at least a daily basis;
- b. Applications and licenses will be backed up whenever there are changes to them; and
- c. The backing up of non-critical data is at the discretion of the data owner.
- d. Backups will be stored off-site in a secure, environmentally-controlled location.

Patch Management and System Updates

The ELC systems are to be maintained with updated security patches or system updates.

Server Security

Servers shall be made secure before placing them into the ELC operational environment and security shall be maintained throughout their lifecycle. In the event the ELC uses a third-party server or cloud-based service for its ELC systems, the ELC shall ensure that the third party server or cloud-based service is secure before placing them into the ELC operational environment and that the third party who owns or its in control of the third party server or cloud-based service properly maintains security throughout their lifecycle of the contract or the state of Florida retention schedule, whichever is applicable.

Cloud Security

Cloud-based systems used to store, process, or transmit Coalition information must be approved by the IT Department. Cloud services must implement appropriate encryption, access controls, audit logging, backup capabilities, and security safeguards.

Mobile Computing

Security controls shall be implemented to mitigate the increase risks posed by the use of laptops and other mobile devices outside of the ELC main or satellite offices or ELC program sites. Those ELC employees are part of the ELC's telework program as set forth in the ELC's Telework Policy and Procedure shall be required to comply with this policy as applicable.

Network Security

Network devices and connectivity components shall be made secure before placing them into the ELC's operational informational technology environment, and security shall be maintained throughout their lifecycle.

Remote Access

Remote access shall mean any access to the office network through a network, device, or medium that is not controlled by the ELC (such as the Internet, public phone line, wireless carrier, or other external connectivity). Security controls shall be implemented to mitigate increased risks posed by allowing remote connectivity to ELC systems.

Electronic Mail

Electronic mail shall be protected from threats and vulnerabilities that can cause system damage, data compromise and business disruption.

Database Security

Securing information, so that it remains consistent, complete and accurate, is essential to the reputation, mission and critical business objectives of the ELC. Information shall remain consistent, complete and accurate.

Electronic Media Management

Electronic media shall be handled, stored and disposed of properly in order to protect the confidentiality of the ELC data, records, files and other information.

Password Management

Passwords are an important aspect of information security. The ELC shall protect access to its systems by ensuring that any passwords used for authentication are properly assigned and protected. The ELC staff shall also comply with requirements for passwords described in the user access management procedures.

Information Technology Asset Management

All information technology assets are tracked for inventory purposes by the Finance/Administration department.

Confidentiality Statement

The provisions of the Florida Public Records Act and other applicable state and federal laws will govern disclosure of any confidential information received by the state of Florida.

The ELC acknowledges each agency, organization or individual receiving confidential and exempt record in order to carry out official functions must protect all records, file data or other information. Those with access to data, records, files or other information other information that is confidential and exempt from disclosure in accordance with federal and Florida law ("Confidential Information") must not permit persons other than those authorized to receive the Confidential Information concerning a Client's personal identification.

ELC staff as well as any other authorized persons or entities as designated by the ELC shall ensure confidentiality and privacy regarding history, records and any discussions relating to the Clients who the ELC or its Contractor, Subcontractors, or Vendors may serve. The very fact that a Client is served by the ELC, its Contractors, its Vendors or other authorized persons or entities as designated by the ELC shall be kept private or confidential unless disclosure is made under for reasons relating to law enforcement, a court order, fulfillment of a statutory requirement, fulfillment of the ELC mission that does not violate applicable law, or upon signed release by the Client. Neither ELC staff or other authorized persons as designated by the ELC shall not disclose any information about a Client, including whether that Client is served by the ELC, its Contractor or its Vendors, or any other authorized person or entity as designated by the ELC to anyone outside of the ELC, without prior approval of the Chief Executive Officer or other persons authorized by the Chief Executive Officer, if the CEO is so authorized to make said disclosure pursuant to applicable federal and Florida law or in accordance with ELC policies, procedures and bylaws.

The ELC, including its employees, subcontractors, agents or any or other authorized persons or entity as designated by the ELC to whom the ELC authorizes to receive or access Confidential Information as stated herein, shall not store, or allow to be stored, any Confidential Information on any portable storage media (e.g. laptops, thumb drives, flash drives, hard drives, etc.) or peripheral device with the capacity to hold information without encryption software installed on devices meeting industry standards (i.e. National Institute of Standards and Technology).

The principle of confidentiality shall be maintained in all programs, functions and activities. ELC staff, its agents, its Contractors, its Vendors or any or other authorized persons or entity as designated by the ELC shall not discuss any Client of the ELC with any unauthorized third party at any time, whether on or off duty while employed or under contract with the ELC. Confidentiality shall be maintained regardless of separation or termination of employment or termination or expiration of any contract with the Contractor, Subcontractor, Vendor or other authorized person or entity as designated by the ELC.

Maintenance

1. The ELC, its Contractors, its Subcontractors, its Vendors and/or any or other authorized persons or entity as designated by the ELC who receive early learning records in order to carry out official functions must protect the data and records in a manner that will not permit the personal identification of a Client by persons other than those authorized to receive the records;
2. The Contractors, Subcontractors, and/or Vendors of the ELC as well as any or other authorized persons or entity as designated by the ELC shall have documented procedures to maintain confidentiality of early

childhood and other confidential records consistent with this policy if said parties handle Confidential Information on behalf of the ELC;

3.

Security Risk Assessments

The Coalition shall periodically conduct cybersecurity and information security risk assessments to identify threats, vulnerabilities, and control deficiencies.

Assessment results shall be reviewed by executive management and used to strengthen security controls and practices.

COMPLIANCE AND MONITORING

1. The ELC, its officers, its ELC staff, its interns, its Members, its agents, its Contractors, its Subcontractors, its Service Providers and its Vendors as well as any other authorized persons or entity as designated by the ELC shall comply with the applicable confidentiality provisions set forth in Florida Statutes as applicable, which includes, but is not limited to those statutes, codes and other regulation that concerns the records of children participating in School Readiness ("SR") and Voluntary Pre-Kindergarten Education (VPK) Programs and shall not release any information regarding any of the ELC Clients, except as specifically authorized by Florida statutes. Failure to abide by the applicable confidentiality requirements as set forth in those applicable Florida statutes may constitute a criminal offense.
2. Monitoring by the ELC will ensure that the ELC's Contractors, Subcontractors, Service Providers and Vendors are in compliance with the following:
 - All confidentiality provisions and the record retention requirements as set forth in Florida and federal statutes, where applicable.
 - All data security measures of the Health Insurance Portability and Accountability Act ("HIPAA").
 - All requirements for the protection and securing of trademarks, patents, and other proprietary information as set forth in Florida and federal statutes, where applicable.
 - Vendors, contractors, consultants, and service providers with access to Coalition information or systems must maintain reasonable cybersecurity controls. The Coalition may require review of cybersecurity policies, security assessments, cyber liability insurance, audit reports, or other documentation before granting access. Any security incident involving Coalition information shall be reported immediately. Shall not use or disclose any information concerning a Client for any purpose not in conformity with state and federal law or regulations except upon written consent of the Client when authorized by law.
 - Shall comply with the Computer-Related Crimes Act, Chapter 815, Florida Statutes and shall demonstrate due diligence in safeguarding the ELC's information resources by establishing policies and procedures for information systems security that contain criteria and standards as set forth in OEL's policies and procedures.

USER ACCOUNT MANAGEMENT PROCEDURES

It is the policy of the ELC to ensure that those electronic accounts used to perform or deliver ELC related-services and assigned to ELC staff or other authorized parties by the ELC's IT department ("user accounts") are standardized in order to minimize the potential exposure of the ELC, which may result from unauthorized user account access. This includes the loss, distribution or unauthorized access or use of sensitive or company

confidential data, intellectual property, damage to public image, damage to critical ELC systems, and other unforeseen damages. As a result, the following procedures will be followed:

1. All ELC staff must read and sign the **Memorandum of Understanding (“MOU”) and Data Security Agreement**, and hereby made a part of this policy and procedure, on an annual basis.
2. User accounts and passwords are the initial line of defense in network security. The Human Resource Manager must approve the creation/change of account(s) for ELC staff by completing the **System User Account Form** and by reference made part of this policy and procedure. The **System User Account Form** shall be submitted to the IT Department for processing by the HR Manager. ELC staff are granted the necessary privileges based on their account settings (fiscal, program operations and administration) to access files on the network server to accomplish day-to-day work. The ELC’s IT department will approve the creation/change of account(s) for authorized persons other than ELC staff by completing the **System User Account Form**.
3. Computer network passwords and user names are provided to ELC staff to prevent unauthorized access to a computer. New users must change their password at their initial logon. Passwords are required to be at least eight (8) characters in length, and contain characters from three of the following four categories: English uppercase, English lowercase characters, Base 10 digits (0 through 9) and Non-alphabetic characters. Passwords to the ELC network are set to automatically expire every 60 days and prompt ELC users to automatically change/reset their passwords. Passwords cannot be reused for at least six (6) changes. ELC users should not reveal their password to anyone including other ELC staff. Multi-factor authentication shall be required whenever technically feasible. Password resets may be required following suspected compromise, security incidents, or elevated risk conditions. Password sharing is prohibited.
4. ELC staff and other authorized persons as designated by the ELC shall understand their responsibility for safeguarding user names and passwords, and immediately notify their supervisor and/or the ELC’s IT Department if they suspect that a password or the system credential has been compromised.
5. All user accounts are automatically set to lockout after three (3) unsuccessful/invalid login attempt. Lockout account can only be reset manually by the ELC’s IT Department. This policy will help prevent attackers from guessing users’ passwords and it decreases the likelihood of successful attacks on the networks.
6. All workstations/laptops are set to automatically lockout (screen saver mode) after twenty minutes of inactivity timeout. ELC staff and other authorized persons as designated by the ELC are recommended to log off from the workstation/laptop when leaving the work area. Workstations/laptops should not be shut down overnight.
7. When an employee is transferred or employment is terminated or the work performed or delivered by an authorized person as designated by the ELC is completed or terminated by the ELC, the user network account will be changed or deactivated immediately. The Human Resources Manager will notify the ELC’s IT department via email or written documentation (i.e. **System User Account Form**) on the day of transfers or termination of employment that require changes to his/her user account.

SECURITY MANAGEMENT/ACCESS CONTROL

The ELC is committed to protect and safeguard all data and electronic information systems from unauthorized use. All ELC staff and other authorized persons as designated by the ELC are assigned a user account and are granted the necessary privileges based on their account settings to access the network and perform their job function.

In order to protect and safeguard all data and electronic information systems from unauthorized use, the following standards/guidelines will be implemented by the ELC's IT Department:

1. Security measures are implemented by only granting specific access privileges to users required to perform their job duties based on the **System User Account Form** request.
2. Data folders are safeguard and can only be accessible based on access privileges
3. Regularly review records of system and security activity such as audit logs and access activity reports. ELC IT Department will perform desktop audit.
4. Regularly review VPN remote access audit log.
5. ELC's IT Department will maintain a listing of ELC staff and other authorized persons as designated by the ELC who have been granted access, and will periodically review access permissions granted.
6. ELC's IT Department will ensure that those granted access to data system have an approved Level II background screening and have received information security training in accordance with ELC protocols.
- 7.
8. Multi-factor authentication (MFA) shall be required for:
 - a. Email systems
 - b. Remote access
 - c. Cloud applications
 - d. Administrative accounts
- e. Systems containing confidential information

SECURITY TRAINING AND AWARENESS

Security training and awareness is very crucial to the safeguarding of ELC information resources. Information security protocol and standards cannot be effective unless all ELC staff and other authorized persons are aware of the importance of data security, understand the ELC security procedures and protocols, and perform required practices. To make information security effective, standards and procedures must be known, understood, believed to be beneficial, and be appropriately and consistently practiced.

Effective information is achieved when it becomes part of everyone's thinking with regard to daily operations and assignments. In order to achieve effective information security and awareness, all ELC users must complete training on ELC data security policies and procedures. This will consist of the following training activities:

2. Data security training and awareness will be provided to all new ELC staff and other authorized persons as designated by the ELC by the ELC's IT Department covering this policy and procedure. Training to new ELC staff must be completed as soon as practical but less than 30 days of new employment. Training to authorized persons other than ELC staff must be completed within 30 days of approval for access to ELC systems.

3. All ELC users must complete an annual data security training program provided by the IT department to refresh their knowledge of data security. In addition, all ELC Staff and other authorized persons as designated by the ELC must annually complete the Florida's Department of Children and Families ("DCF") Online Security Awareness Training.
4. All ELC Staff and other authorized persons as designated by the ELC must sign an annual agreement that they understand the ELC data security policies and procedures within the ELC computing resources policy and that they will abide by them (**Information Security Training Acknowledgement Form**).

ELECTRONIC MAIL

For purposes of this policy, electronic mail shall mean point-to-point messages, postings to newsgroups and list serves and any electronic messaging involving computers, computer networks or ELC systems. Unencrypted transfer of confidential information by e-mail is strictly prohibited. The ELC complies with requirements for antivirus programs and other required protection programs and protocols as described in OEL's IT Security Policy.

Only electronic mail that is related to ELC business is acceptable for use with the ELC.

The examples below are considered inappropriate and unacceptable use of electronic mail. In general, electronic mail should not be used for the initiation or re-transmission of:

- Chain mail that misuses or disrupts resources (i.e. electronic mail sent repeatedly from user to user, with requests to send to others);
- Harassing or hate mail (i.e. any threatening or abusive electronic mail sent to individuals or organizations that violates ELC rules and regulations and this policy);
- Virus hoaxes;
- Spamming or electronic mail bombing attacks (i.e. international electronic mail transmissions that disrupt electronic mail service);
- Sending or forwarding junk mail (i.e. unsolicited electronic mail that is not related to ELC business and which is sent without a reasonable expectation that the recipient would welcome receiving it);
- Any actions that defraud another or misrepresent or fail to accurately identify the sender;
- Sending copies of documents in violation of copyright laws;
- Inclusion of the work of others into electronic mail communications in violation of copyright laws;
- Use of electronic mail to harass, intimidate or defame others or to interfere with the ability of others to conduct ELC business;
- Use of electronic mail systems for any purpose restricted or prohibited by law, statute, ordinance or regulations;

- “Spoofing,” (i.e. constructing an electronic mail communication so that it appears to be from someone else);
- “Snooping,” (i.e. obtaining access to the files or electronic mail of others for purpose of satisfying idle curiosity);
- Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmission without proper authorization;
- Electronic mail or communications that attempt to hide the identity of the sender, or represent the sender as someone else from another entity; and
- Any other electronic communication that violates this policy, ELC Employee Handbook, or any other law, statute, regulation or ordinance.
- Political or lobbying activities
- Personal business or commercial activities

DATA BACKUP

The backup and maintenance of data is critical to the viability and operations of ELC, and it is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis. This policy is designed to protect data and to ensure it is not lost and can be recovered in the event of a hardware failure, destruction of data, or disaster. The ELC complies with requirements for data backups described in OEL’s IT Security Policy.

To comply with this policy, the following standard procedure was put in place to ensure proper data backup:

Software:

Recognized industry approved software is used to backup all ELC data on a nightly basis. Software can be used to restore data in the case of an emergency.

Schedule:

An automatic full data backup is performed online daily and saved to a secure off-site location. A network attached storage device is also used to generate data backup locally. The ELC’s IT Department monitors the success of these backups on a daily basis and periodically reviews/updates to policy and processes for changes in operations, identifies important data files, periodically performs testing and restore backup files, reviews backups and performs regular backups.

MEDIA DEVICES/PHYSICAL/SYSTEM/DATA SECURITY

It is the policy of ELC to ensure the protection of Confidential Information. The purpose of this specific procedure is to establish guidelines and requirements to ensure the appropriate protection of ELC systems. In doing so, the following steps must be implemented:

1. The ELC's IT Department is required to establish appropriate user privileges, monitor access control logs and similar security actions for the systems he/she administers.
2. Computer resources and equipment must be stored in secure locations (server room, wiring closets, etc.) with restricted access.
3. If the ELC determines that an item of grant-purchased property is no longer needed or required by the ELC, its agents, its Contractors, its Subcontractors or its Vendors is obsolete, is not usable, or is not economical or efficient to use, the ELC may surplus or dispose of the property in accordance with OEL surplus or disposal of grant-purchased property procedures or the ELC applicable disposition of property policy and procedure, whichever is applicable.
4. Magnetic media such as hard drives, diskettes, universal serial bus ("USB") flash drives, thumb drives or tapes must be erased and destroyed by ELC's IT Department before disposal.
5. Uninterruptible power supply ("UPS") is required for networking devices and server(s).
6. Only the ELC's IT Department staff shall install applications on a server or workstation.
7. Operating systems and system applications must be kept current.
8. ELC computer network must be secured and protected with a network based firewall and antivirus.
9. All electronic ELC work (files/documents) must be stored on server.
10. Servers must not be used for general purposes computing such as web browsing or reading emails and must be strictly used for its intended purpose.
11. Equipment checked out to ELC staff or other authorized persons as designated by the ELC must be utilized for ELC related business. Use of ELC equipment for non-ELC business is prohibited under ELC policies and procedures. Equipment lost or stolen while in the personal possession of an employee or other authorized persons as designated by the ELC is the responsibility of the employee or other authorized persons and must be reported to their supervisor, if applicable and the IT department immediately. ELC will review any instances of theft or foul play pertaining to the equipment. All ELC staff or other authorized persons as designated by the ELC requesting the use of a laptop or any other equipment owned by ELC must complete and sign an **Equipment Checkout Authorization Form**.

The ELC complies with the requirements described in OEL IT Security Policy regarding, physical and environmental security.

ANTIVIRUS

To assure continued uninterrupted service and to minimize the impact of computer viruses on ELC systems, all ELC servers, workstations, laptops, as well as any computers used for remote access to connect to the ELC network must have antivirus software installed and kept up to date. All disk drives, USB flash drives, thumb drives downloaded files, etc., must be scanned before using them on computers, laptops, and servers.

In order to protect the ELC systems from viruses, malware, spam or other internet attacks, the following steps/actions must be taking by all ELC staff or other authorized persons as designated by the ELC:

1. Never install software on ELC computers without permission from the IT Department.
2. Never download files from unknown or suspicious sources.
3. ELC staff should not remove or disable antivirus or other protection software from any ELC computers.
4. If a computer virus, malware or other malicious program is suspected to have infected ELC systems, immediately notify your supervisor and the ELC's IT Department.
5. ELC staff or other authorized persons as designated by the ELC are responsible for taking appropriate precautions to avoid introducing viruses, malware or other malicious programs into the ELC computing environment.
6. Antivirus software is set to update automatically as new virus definitions are made available by the ELC's vendor for said software.
7. ELC's IT Department is responsible for deploying antivirus agent to each ELC network computers from the server and to regularly monitor the ELC antivirus console installed on the server to verify that antivirus protects all computer systems:
 - a. Antivirus software applies to all servers, workstations, and remote access computers;
 - b. Every server or computer that contains OEL data or conducts and form or OEL business runs antivirus software;
 - c. Antivirus software protects data, scan documents, attachments, emails and internet sites before use by staff; Antivirus program scan portable media devices;
 - d. Documentation is maintained to verify the purchase and installation of antivirus software.

MOBILE COMPUTING

The use of laptop computers and mobile devices provide flexibility and enhanced communications that allow ELC staff or other authorized persons as designated by the ELC to be more productive. However, the use of these devices outside of the offices of the ELC poses risks to those devices and the information they contain. These devices may also present a hazard to the ELC data systems upon their return to the office (for example, by spreading a virus that was obtained outside the office). These devices have the capability for direct connectivity to the internet or other networks outside of the ELC network which lack the protections afforded by ELC network firewalls and other perimeter protections. Therefore, additional security measures must be implemented to mitigate increased security risks presented by mobile computing. This procedure establishes procedures for

mobile computing and applies to all laptops and other mobile computing devices that are used to store or process ELC data. Coalition-owned mobile devices shall be managed through an approved Mobile Device Management (MDM) platform. The Coalition reserves the right to remotely lock, locate, or wipe Coalition-owned devices that are lost, stolen, compromised, or no longer authorized.

To protect the ELC data systems from the security risks mobile devices present when used, the following standards/guidelines must be implemented by ELC staff or other authorized persons as designated by the ELC:

1. Laptops and other mobile computing devices must be inventoried by the Finance/Admin department and tracked by the IT department personnel.
2. Laptops must have antivirus installed with current updated definitions. The firewall must be enabled on the laptop computer.
3. Confidential information placed on mobile devices must be protected against unauthorized access and encrypted. Storage of Confidential Information on any mobile device is prohibited by the ELC.
4. Mobile computer users are responsible for backing up their data that is stored on the mobile computer on a regular basis.
5. ELC staff are responsible to take reasonable precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.
6. ELC staff and other authorized persons as designated by the ELC must immediately report their supervisor and/or IT department any loss, theft, tampering, unauthorized access, or damage of any mobile device.
7. All ELC staff or other authorized persons requesting the use of mobile devices owned by ELC must complete and sign an **Equipment Checkout Authorization Form**. Any ELC staff or other authorized persons as designated by the ELC assigned an ELC mobile device must also complete an **Employee Receipt of Property Form**. The Employee Receipt of Property Form will be kept by Human Resources Manager for the ELC.
8. ELC's IT Department is responsible for auditing the use of ELC mobile computing devices to ensure compliance with the procedures and guidelines set forth in this protocol.
9. Equipment checked out to ELC staff or other authorized persons as designated by the ELC must be utilized for ELC related business.

REMOTE COMPUTING

Remote access to Coalition information systems provides operational flexibility and supports the efficient delivery of services. However, remote connectivity increases the risk of unauthorized access, data interception, and cybersecurity threats. Therefore, appropriate security controls must be implemented to protect Coalition information resources accessed from outside the Coalition's network environment. This protocol establishes requirements for all remote access connections to Coalition systems and information resources. The purpose of this protocol is to safeguard the confidentiality, integrity, and availability of Coalition information and to reduce

the risk of harm to Coalition systems, operations, and data. Only Coalition-approved and managed devices may connect to Coalition systems containing confidential or sensitive information. Multi-factor authentication shall be required for remote access whenever technically feasible. Remote access activity may be logged, monitored, and audited to support security and compliance requirements.

The following security measures must be implemented to mitigate the increased security risks presented by remote computing:

1. All ELC staff by default will have account settings set to deny remote access. Only upon request will the account settings be changed to allow remote access. ELC staff or other authorized persons as designated by the ELC must read and sign a **Remote VPN Access Form**. Only upon the approval of the Remote Access VPN Request Form will the employee or other authorized persons as designated by the ELC be allowed to remote VPN by the ELC's IT department.
2. All remote connectivity must be authenticated. Confidential Information transferred over a remote access connection must be encrypted to protect it from unauthorized disclosure.
3. All data security policies for use in the ELC office environment must also be observed when using or connecting to ELC resources while outside the ELC office environment.
4. Confidential Information is not to be stored on any non-ELC computers. It is the responsibility of ELC staff to ensure that their access devices and remote connections are not used by unauthorized persons (including family members).
5. ELC remote users may not change operating system configurations, install new software, alter equipment or download software from systems outside of ELC network onto ELC remote access computers.
6. To prevent unauthorized users from accessing Confidential Information, ELC remote users must log out up after completing a remote session.
7. ELC remote users are responsible for complying with the procedures and guidelines set forth in this protocol; protecting their remote access credentials and devices from disclosure to, or use by, unauthorized persons; and immediately reporting any suspected unauthorized use of their remote access account or any damage to or loss of ELC computer hardware, software, or data that has been entrusted in their care.
8. The ELC's IT Department is responsible for auditing the use of remote access to ensure compliance with the procedures and guidelines set forth in this protocol. The ELC's IT department will regularly review remote access audit log.
9. Personal home computers are prohibited from connecting to ELC network.

USE OF INTERNET/WORLDWIDE WEB

The internet/worldwide web (collectively the “Internet”), can be a valuable research tool and resource for ELC and its ELC staff. However, as with all electronic communications and services, the use of the internet is subject to abuse.

Subject to all policies and prohibitions contained herein, those contained in the ELC Employee Handbook, and as otherwise set forth under relevant laws, statutes, regulations and ordinances, ELC staff or other authorized persons as designated by the ELC may utilize the internet to conduct ELC business and for limited personal use. However, in utilizing the Internet, ELC staff or other authorized persons as designated by the ELC must remain cognizant that:

1. Any messages or information sent by an employee to one or more individuals via an electronic network (e.g., bulletin board, on-line service, or Internet) are statements identifiable and potentially attributable to ELC. While some users include personal “disclaimers” in electronic messages, it should be noted that there would still be a connection with ELC, and the statement might still be legally imputed to ELC. All communications sent by ELC staff via a network must comply with this and other ELC policies, and may not disclose any confidential or proprietary information.
2. Network services and internet sites can and do monitor access and usage and can identify at least which Early Learning Coalition of Broward County/entity (and often which specific individual) is accessing their services. Thus, accessing a particular bulletin board or website leaves ELC-identifiable electronic “tracks” even if the employee merely reviews or downloads the material and does not post any message.
3. As previously noted, ELC will allow limited use of electronic mail for personal reasons for ELC staff. Subject to the restrictions noted in this policy, ELC staff may also access the internet for personal reasons on a limited basis.

Screensavers

ELC staff may retain approved screensavers on the hard drives of their computer, subject to the provisions and restrictions of this policy.

Sensitive Information

ELC staff or other authorized persons as designated by the ELC must be cognizant that certain information about providers and individuals affected by our programs is confidential by law or is otherwise sensitive information. Information such as social security numbers, financial information or private information concerning children, must be guarded and protected by all ELC staff or other authorized persons as designated by the ELC.

Games/Purchasing Private Goods and Services

ELC staff may not use ELC systems to access, play games, contests, audio, video or any other forms of entertainment. Similarly, ELC staff or other authorized persons as designated by the ELC may not use the ELC systems to purchase personal goods and services over the Internet.

VIOLATIONS OF POLICY

Accidental Violation Of Policy

Any ELC staff or other authorized persons or entity as designated by the ELC who believes that he/she has inadvertently or accidentally violated the provisions of this policy must disclose the same in writing to their supervisor within one (1) business day of such violation.

Requirements of Managers and Supervisors

Managers and supervisors are responsible for ensuring policy compliance and for taking appropriate action when violations are identified.

Reporting Violations

ELC staff or other authorized persons as designated by the ELC must report any violations of this policy to Human Resources and in accordance with ELC policies and procedures. ELC may also refer suspected violations of applicable law to appropriate law enforcement agencies.

No Duty to Defend

ELC reserves the right not to defend any employee or other authorized persons or entity as designated by the ELC for any action brought by any person or entity for violation of any law, statute, regulation or ordinance committed by such employee or other authorized persons or entity using the ELC systems. In addition, ELC reserves the right to seek indemnification or subrogation from any employee or other authorized persons or entity as designated by the ELC in any action to which ELC is made a party based upon the employee's violation of any law, statute, regulation or ordinance.

APPLICABLE LAWS

The ELC will comply with all applicable federal and Florida laws governing data security, breach of security, reporting incidents and confidentiality.

In the event this policy and procedure, whether in whole or in part, creates an unallowable conflict with applicable federal or Florida statute, codes or rules or the Grant Agreement, the applicable federal or Florida statute, codes or rules and Grant Agreement will prevail.

EXHIBIT A - MEMORANDUM OF UNDERSTANDING - OEL

The Office of Early Learning and the local Early Learning Coalitions recognize that the full participation of the coalitions as a partner is critical to the success of the school readiness programs and the sharing of data between all parties is contemplated in the School Readiness Act. Thus, OEL hereby agrees to make available to the early learning coalitions and their agents, for the limited purpose of performing their public duties, school readiness programs information that includes, but is not limited to, data which is maintained in the Enhanced Field System ("EFS"), Statewide Reporting System ("SRS"), the Single Point of Entry/Unified Waiting List ("SPE/UWL") system, SharePoint and any replacement systems providing the same school readiness data.

I. Designation of System Administrator and Security Officer

Each Early Learning Coalition will appoint a System Administrator and a Security Officer. Each Early Learning Coalition will notify the Information Systems Security Officer for OEL in writing who the designated System Administrator and Security Officer will be. OEL encourages each early learning coalition to designate separate individuals for each role.

The Early Learning Coalitions; their System Administrators, Security Officers, staffs, and employees; and the early learning coalitions' participating partners, contractors, subcontractors, any subsequent subcontractors, and their employees agree to maintain the confidentiality of school readiness data to include, but not be limited to, social security numbers, parent and child information, payments, childcare provider information, household demographic information, resource and referral information, and all related information pursuant to State and Federal regulations unless such information has been exempted from non-disclosure for business purposes in accordance with State or Federal law. Such information may be released if a lawful and proper authorization has been submitted by a participant of the program or a childcare provider.

The early learning coalitions will ensure that their System Administrator, Security Officers, staff, and employees; and the early learning coalitions' participating partners, contractors, subcontractors, any subsequent subcontractors, and their employees are sufficiently trained relative to non-disclosure and confidentiality regarding applicable school readiness programs. The early learning coalitions will assign access to the school readiness data systems only to early learning coalition and Office of Early Learning staff, contractors, subcontractors and subsequent subcontractor employees who have been properly trained by the early learning coalition regarding the confidentiality of school readiness records and who have completed and signed the "Data Security Agreement".

The early learning coalitions will require the System Administrator, Security Officer, staff, contractors, subcontractors, and any subsequent subcontractors and their employees who have access to confidential information to sign and comply with the "Data Security Agreement." The ELC will maintain these forms on file subject to inspection by the Office of Early Learning.

Early Learning Coalitions will advise their System Administrator, Security Officer, staff, contractors, subcontractors, and any subsequent subcontractor and their employees that they are not to make copies of confidential documents or to access, allow access to and/or use any confidential information for personal intent or any purpose other than

in performance of their official duties.

II. Confidentiality and Public Access

All documents, papers, computer files, letters or other materials made or received in conjunction with the Agreement will be subject to the applicable legal requirements for maintaining confidentiality in conformance with Federal, State and local laws.

Public access to these records will be in accordance with Chapter 119 of the Florida Statutes and all other applicable laws or regulations.

Although the early learning coalitions' staff, contractors, subcontractors and their employees may obtain access to information that is otherwise confidential, that access does not alter the confidential nature of the information. It is incumbent upon the early learning coalitions; their System Administrators, Security Officers, staffs, and employees; and the early learning coalitions' participating partners, contractors, subcontractors, any subsequent subcontractors, and their employees to maintain confidentiality requirements.

Any requests for release of information covered under this Agreement by parties other than those specified in this Agreement will be referred to the Office of Early Learning.



Data Security and Systems Policy and Procedures

DRAFT PENDING APPROVAL

October 3, 2019

Presented to

Governance on 9/24/26

Board on 10/05/26

TABLE OF CONTENTS

STATEMENT OF POLICY 3

PURPOSE..... 3

STATEMENT OF PROCEDURE..... 5

DEFINITIONS 5

APPLICATION OF FEDERAL AND FLORIDA’S DISCLOSURE AND PUBLIC RECORDS LAWS..... 7

USE OF ELC SYSTEMS..... 7

ELECTRONIC TRANSMISSION..... 9

COMPLIANCE AND MONITORING 155

USER ACCOUNT MANAGEMENT PROCEDURES 16

SECURITY MANAGEMENT/ACCESS CONTROL..... 17

SECURITY TRAINING AND AWARENESS..... 17

ELECTRONIC MAIL 18

DATA BACKUP..... 19

MEDIA DEVICES/PHYSICAL/SYSTEM/DATA SECURITY.....**ERROR! BOOKMARK NOT DEFINED.**

ANTIVIRUS 20

MOBILE COMPUTING 20

REMOTE COMPUTING 21

USE OF INTERNET/WORLDWIDE WEB..... 23

EXHIBIT A - MEMORANDUM OF UNDERSTANDING - OEL..... 24

ELC Policy Name: **Data Security and Systems Policy and Procedure**

ELC Policy No.: **IT-POL-001**

Approval Date: **Pending Board Approval**

STATEMENT OF POLICY

As part of its mission, the Early Learning Coalition of Broward County, Inc. ("ELC") maintains computers, servers, cell phones, data systems and a secure network. These computing resources are intended for ELC-related purposes. For purposes of this policy and procedure, "ELC systems" shall mean all computing, data, network, platforms and web/cloud based resources or systems including, but not limited to, the use of electronic mail, internet, intranet, web pages, video communication, portable devices (i.e. cell phones, jump/USB drives, storage media, etc.), computer software, computer hardware and cloud/server based storage, messaging, databases, or repositories, whether internal or external, that are owned, leased or controlled by the ELC and/or OEL, its agent(s) or other authorized third parties contracted with the ELC, that the ELC utilizes to store, transmit, distribute, create, delete or access data, records, files, documents, materials or other information that is the property of or has been licensed to the ELC and/or the Office of Early Learning ("OEL").

ELC staff have access to one or more forms of data systems and ELC encourages the use of approved data systems and associated services and products as they make communication more efficient and effective, and because they are valuable sources of information. However, all computer systems provided by ELC for employee use are the property of ELC and their purpose is to facilitate ELC business.

This policy expresses the ELC philosophy and sets forth general principles to be applied in the use of ELC systems. The ELC expects its staff to understand that they are to use good judgment when it comes to using the ELC systems. This policy is designed to provide guidance for basic principles and premises of the use of the ELC systems for the transaction of ELC business.

All ELC staff, contracted employees, Vendors, Contractors, Subcontractors, and others doing business with the ELC are expected to comply with all provisions of this policy as well as applicable federal and Florida statutes, rules and regulations. The aforementioned parties are also expected to comply with the applicable authoritative citations with the most recent funding agreement between the ELC and the applicable governing agency for the ELC ("Grant Agreement").

PURPOSE

The purpose of the data security policy is to define, develop and document the information protocols, standards, and procedures that support the ELC goals and mission to ensure that all Personal Identifiable Information (PII), assessment, and health data of all families and children served are guaranteed to be safe and confidential and release of data is in accordance with the guidance of Office of Early Learning ("OEL").

Data security policies/protocols, standards and procedures represent the foundation for ELC information security system. The policies serve as overarching guidelines for the use, management, and implementation of information security throughout the organization.

SCOPE

The Data Security Policy is an official directive of the Chief Information Officer (“CIO”) as approved by the Board. This policy applies to all employees of the ELC, its Contractors, its Vendors, its Service Providers, and any other authorized persons or entities designate by the ELC and its respective ELC systems that are:

- Accessed and/or stored on ELC premises or on the cloud;
- Accessed using ELC or ELC funded data systems;
- Accessed using ELC or ELC funded paid access methods;
- Accessed using ELC data systems from a remote location;
- Used in a manner which identifies the individual with ELC; and/or
- Used for the transaction of ELC business, including data systems that are owned by ELC, as well as those which are owned by the user and/or any other person or entity.

Board Chair’s Signature: _____

Date Signed: _____

STATEMENT OF PROCEDURE

DEFINITIONS

1. **Board** shall have the same meaning as it does in the ELC bylaws.
2. **Artificial Intelligence (AI)** means computer systems capable of performing tasks that typically require human intelligence, including generative AI, machine learning, predictive analytics, natural language processing, and large language models.
3. **Breach** shall mean a confirmed event that compromises the confidentiality, integrity, or availability of information or data (Ch. 282.0041, F.S.)
4. **Breach of Security** shall mean any unauthorized access of data containing personal information. A breach of security shall mean an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information ("PHI"), personally identifiable information ("PII"), Protected personally identifiable information ("PPII"), trade secrets or intellectual property. Good faith access of data containing personal information by an employee or agent of ELC does not constitute a breach, provide the information is not used for a purpose unrelated to the agreement, task or subject to further unauthorized use (Ch. 501.171, F.S.).
5. **Chair** shall have the same meaning as it does in the ELC bylaws.
6. **Client** shall mean the intended recipients of the ELC and/or Florida's Office of Early Learning ("OEL") grant related activities, services or funding, including, but not limited to the ELC Voluntary Pre-Kindergarten ("VPK") or School Readiness ("SR") programs and services such as children, parents and legal guardians.
 - 1.
7. **Cloud Service Provider** means a third-party organization that hosts, processes, transmits, or stores Coalition information using internet-based services.
8. **Confidential Information or Confidential** shall mean records, systems, specific records or individually identifiable data that by law are not subject to public disclosure pursuant to applicable federal and Florida statutes, codes, and other regulations. When applicable, this definition or any reiteration of it covers all documents, papers, materials computer files, letters, and all other notations of records, data or other information that are designed by law or contract, whichever is applicable, as confidential, including but not limited to those items that may be considered proprietary information, intellectual property, or trade secrets belonging to the ELC, OEL or a third party. Furthermore, the term "confidential" covers the verbal conveyance of data or information that is designed by law or contract confidential.
9. **Contractor** shall mean those eligible licensed entities that contract directly with the ELC to provide School Readiness or Voluntary Pre-Kindergarten services and/or programs in accordance with Florida Statutes and provides monitoring, investigations and/or other oversight functions on behalf of the ELC to Service Providers. For purposes of this policy and procedure, the term "**Contractor**" shall have the same meaning as the term "**lead agency**" or "**sub-recipient**" in any statewide agreement(s) created by the Office of Early Learning, any other governing state agency or authority for the ELC, any applicable federal or Florida statutes, or within any contract or agreement with a third party concerning VPK or SR services.

10. **ELC** shall mean the Early Learning Coalition of Broward County, Inc. For purposes of this policy and procedure, the term “**Coalition**” shall have the same meaning as the term “**ELC**”.
11. **ELC staff** means those persons directly employed by the ELC.
12. **Member** shall have the same meaning as it does in the ELC bylaws.
13. **Multi-Factor Authentication (MFA)** means an authentication method requiring two or more verification factors before granting access to a system or application.
14. **Personally Identifiable Information (“PII”)** shall mean information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.
15. **Protected Personally Identifiable Information (“PII”)** shall mean information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
16. **Public Records** shall mean any hard copy or electronic copies of records made or received by any public agency in the course of its official business. Records such as policies, meeting minutes, files, program results, computer records, emails, text messages and social media accounts are all available for inspection unless specifically exempted in state statute.
17. **Secure File Transfer Protocol (“SFTP”)** shall mean a secure method of transferring files between two remote systems.
18. **Security Incident** means a violation or imminent threat of violation, whether such violation is accidental or deliberate, of information technology security policies, acceptable use policies, or standard security practices. An imminent threat of violation refers to a situation in which the state agency has a factual basis for believing a specific incident is about to occur. A breach includes a confirmed event that compromises the confidentiality, integrity, or availability of information or data. (Ch. 282.0041 F.S.).
19. **Service Providers** shall mean an eligible public school, private faith-based, licensed or license-exempt child care entity that has provider agreement with the ELC and/or a Contractor to provide Voluntary Pre-Kindergarten (“VPK”) or School Readiness (“SR”) program services directly to children in Broward County in accordance with Florida Statutes. For purposes of this policy and procedure, the term “**Service Provider**” shall have the same meaning as the term “**Provider**” in any statewide agreement(s) for VPK and SR created by the Office of Early Learning (“OEL”), any other governing state agency for the ELC, any applicable federal or Florida statutes, or within any contract or agreement with a third party concerning VPK or SR services.
20. **Subcontractor** shall mean those persons or entities that have a contract with the ELC or a Contractor and are retained to perform either a portion or all of the SR and/or VPK program related services on behalf of the Contractor or ELC under those original contracts. For purposes of this definition, “SR and/or VPK program related work” shall mean services that would not fall under the definition of a “**Vendor**” such as instructional, client engagement, monitoring, and reporting. This definition shall also exclude those person or entities that deliver or perform professional services. For purposes of this definition, “professional services” shall mean accounting, finance, audit, legal or licensed healthcare related services.

21. Vendor shall mean a dealer, distributor, merchant or seller who provides goods and services within business operations; provides similar goods or services to many different purchasers; operates in a competitive environment; provides goods or services that are ancillary to the operation of the federal program; and is not subject to compliance requirements of the federal program. For purposes of this policy and procedure, the term **“Consultant”** shall have the same meaning as the term **“Vendor”**.

APPLICATION OF FEDERAL AND FLORIDA’S DISCLOSURE AND PUBLIC RECORDS LAWS

This policy shall be subject to those applicable federal and Florida statutes, codes and regulations governing access, disclosure, distribution, alteration, retention, destruction and maintenance of public records, which would include, but not be limited to Florida’s public records statute, Chapter 119. Records requests shall be done and this policy and procedure shall be subject to the ELC’s Public Records Policy and Procedure. In the event there is an unallowable conflict between the ELC’s Public Records Policy and Procedure and this policy and procedure, the ELC’s Public Records Policy and Procedure shall control.

Electronic mail created or received by ELC staff or other authorized persons or entities as designated by the ELC in connection with official business, which perpetuates, communicates or formalizes knowledge, is subject to the public records law and is open for inspection unless specifically exempt by law or ordered by a court of law not to be disclosed by the ELC. If your electronic mail falls within the definition of a public record, you may not delete it except as provided in the ELC’s records retention schedule as set forth in the ELC’s Records Management Policy and Procedure. All ELC-issued cellular phones are subject to public records request per Florida Statutes Chapter 119.

USE OF ELC SYSTEMS

The ELC systems may not be used for knowingly transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature, or which are derogatory to any individual or group, or which are obscene, pornographic, suggestive or inappropriate communications, or are of a defamatory or threatening or offensive nature, or for “chain letters” or for any other purpose which is illegal or against ELC policy or contrary to the interest of ELC by ELC staff, its volunteers, its interns, its contracted third parties, or its Board Members.

The ELC systems are primarily for ELC business use. Limited, occasional or incidental use of the ELC systems for personal, non-business purposes is understandable, as is the case with personal phone calls. Such limited, occasional, or incidental use of ELC systems is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user’s job or other ELC responsibilities, and is otherwise in compliance with this policy and procedure. However, subject policies set forth herein, the ELC Employee Handbook and as otherwise required by law, ELC staff need to demonstrate a sense of responsibility and may not abuse the privilege.

To safeguard data and confidential information, ELC prohibits the use of personal data storage devices on the network in order to ensure conformity and that every employee is only using an ELC approved secure-encrypted storage media or equipment (e.g. flash drives, thumb drives, etc.). ELC staff or other authorized persons or entities as designated by the ELC are not allowed to use personal computers in order to access mission critical servers/files systems, databases or other platforms, but may be given secure access to the Internet via a secured guest Wi-Fi network, which does not allow users access to ELC internal network.

Electronic information created and/or communicated by an employee that is not saved or backed-up on the ELC's server or any third -party database or cloud system utilized by the ELC, will not generally be monitored by ELC. However, the following conditions should be noted:

1. The ELC reserves the right to monitor usage patterns for all of the ELC systems.
2. The ELC also reserves the right, in its discretion, to review, monitor, audit, intercept, access, disable and/or disclose any employee's electronic files and messages and usage and/or the hard drive, portable devices, software, hardware or any other computing resource of any ELC employee for any lawful purpose including, but not limited to, ensuring that ELC resources are being used in compliance with applicable federal and Florida laws as well as in accordance with the ELC policies and procedures.
3. ELC staff or other authorized persons as designated by the ELC should not assume that electronic communication or data stored on in accordance with this policy and procedure are totally private and confidential and should take proper steps to transmit highly sensitive or personal information in accordance with this policy and procedure and applicable law. ELC staff should not assume that ELC systems are their personal property.
4. ELC staff or other authorized persons as designated by the ELC must respect the confidentiality of other people's electronic communications and may not attempt to "hack" into other systems or other people's logins, or "crack" passwords, or breach computer or network security measures or otherwise access the electronic communications in an unauthorized or unapproved manner. ELC staff or other authorized persons as designated by the ELC may not monitor electronic files or communications of other ELC staff or third parties except under the explicit direction of the Chief Information Officer or Chief Executive Officer of the ELC.
5. The ELC reserves the right to remove ELC system privileges from an employee or other authorized persons as designated by the ELC.
6. The ELC systems are not to be used for personal commercial purposes or for personal, financial or other gain.
7. No employee or other authorized persons as designated by the ELC will knowingly create access to ELC systems in such a way to bypass ELC security systems.
8. No employee or other authorized persons will use ELC systems for illegal activities.
9. All ELC staff and other authorized persons will do their best to ensure all software or data is free of any viruses, malware, trojans or other harmful programs before it is installed or loaded on the ELC data network. Any detection of any virus malware, trojans or other harmful programs must be reported immediately to the ELC's Information Technology ("IT") Department. ELC staff will be trained on a regular basis to make they are aware of data security threats.
10. Violation of this policy and/or violations of applicable laws, statutes and ordinances may result in loss or limitations on use of information technology resources related to the ELC systems as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.
11. Contractors and Vendors must sign a non-disclosure agreement protecting any confidential data to which the Contractor or Vendor requires access. A Contractor or Vendor shall ensure that the requirement to comply fully with this policy and procedure is included any agreement or contract with any Subcontractor if said Subcontractor is utilized to perform or deliver, whether in whole or in part, any ELC-related service or work done

by the Contractor or Vendor. The Contractor or Vendor shall be responsible and shall be held liable for the violation of this policy and procedure by any Subcontractor utilized to perform or deliver, whether in whole or in part, any ELC-related service or work done by the Contractor or Vendor. Persons or entities authorized to confidential data as described in the policy and procedure will be required to sign a non-disclosure agreement protecting any confidential data to which the person or entity may requires access.

ARTIFICIAL INTELLIGENCE (AI) SYSTEMS

The use of Artificial Intelligence (AI), Generative AI, Machine Learning, and Large Language Model technologies must comply with the Coalition's Artificial Intelligence Acceptable Use Policy.

Users shall not enter confidential information, personally identifiable information (PII), protected health information (PHI), personnel information, provider information, financial information, or other non-public Coalition information into publicly accessible AI tools unless specifically approved by the Chief Information Officer or Information Security Manager.

AI systems connecting to Coalition data repositories, email systems, cloud environments, or business applications shall undergo a security review before implementation.

AI-generated content must be reviewed by an authorized individual before use in official Coalition operations, communications, compliance activities, or decision-making.

ELECTRONIC TRANSMISSION

Transmission Procedures

The ELC and its Contractors and its Vendors as well as any other authorized person as designated by the ELC must safeguard private and confidential data such as names, addresses, social security numbers, and federal employment numbers. Unencrypted transfer of private and confidential information by e-mail or mobile devices (flash drives, thumb drives, cell phones or laptops) is prohibited. This prohibition applies to submissions to the Office of Early Learning ("OEL"), Department of Education ("DOE"), as well as transmissions among contractors, vendors and sub-recipients. All transmission of confidential data must be secured. The ELC's IT Department strongly encourages staff and any other authorized person as designated by the ELC to transmit confidential data via OEL's SharePoint site, Secure File Transfer Protocol ("SFTP") site or via any third-party cloud system utilized by the ELC which would include but not be limited to Sharefile. The ELC currently complies with requirements for restrictions on access to sensitive or confidential data as described in OEL's IT Policy and Program Guidance.

Examples of secure transfer of confidential data, records and files include but are limited to the following:

- Encryption of a file with a program.
- The use of last names plus the last four digits of social security numbers.
- Ensure that sensitive paperwork is secured and not in view of unauthorized persons
- Transmit data behind a firewall.
- Transmit data via SFTP
- Transmit via any third-party cloud system utilized by the ELC which would include but not be limited to Sharefile

The following definitions and information can be found in the applicable OEL program guidance regarding records confidentiality:

Acceptable Use of Information Resources

Individuals using information resources or data belonging to a governmental or quasi-governmental entity or agency shall act in a legal, responsible, and secure manner, with respect for the rights of others.

Information Resources Classification

All information resources (including data and systems) shall be identified, categorized and protected according to their level of confidentiality. All files should be stored and filed appropriately on the ELC server (whether it is a physical or web/cloud-based server).

Security Training and Awareness

The ELC information technology and security policies, procedures, and protocols shall be communicated to all ELC staff or other authorized persons as designated by the ELC, and shall be available for reference. Any changes to those information technology and security policies, procedures, and protocols will be discussed at ELC staff meetings.

Incident Reporting

ELC staff, Contractor, Vendors, Service Providers, Subcontractors and other authorized persons as designated by the ELC are required to report suspected security incidents, unauthorized disclosures, or security breaches in accordance with the ELC Incident Reporting Policy and Procedure. Incident reports should be reported and forwarded to the ELC's IT Department immediately. Within 24 hours of the incident, the ELC shall provide written notification to the Office of Inspector General and the Information Security Manager.

Written notification to OEL must identify the following:

1. The nature of the unauthorized use or disclosure
2. The confidential information used or disclosed
3. Who made the unauthorized use or received the unauthorized disclosure
4. What the ELC has done or shall do to mitigate any harmful impact of the unauthorized use or disclosure and;
5. What corrective action the ELC has taken or shall take to prevent similar future unauthorized use or disclosure incidents.
6. Provide any additional information as reasonably requested by OEL.

See Incident Reporting Policy for further information.

Incident Response

The ELC shall be able to respond to computer security-related incidents in a manner that protects its own information and helps to protect the information of others that might be affected by the incident.

Incident response and reporting requirements can be found in Breach of Security/Confidentiality section of the OEL Grant Agreement. In the event there is an unallowable conflict between the Grant Agreement and the ELC's Incident Reporting Policy and Procedure, the Grant Agreement shall prevail.

Security System Plans

The ELC's computer system shall contain a firewall which shall monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

Monitoring the Adequacy of System Performance and Hardware

The ELC shall periodically monitor the following:

- (1) appropriateness of access privileges assigned to users of certain systems and hardware;
- (2) periodically reviewing the appropriateness of access privileges assigned to users of certain systems;
- (3) performance of system hardware and capacity-related issues; and
- (4) ensuring appropriate backup procedures and disaster recovery plans are in place.

Contingency Planning

Alternate modes of operation exist to ensure continuity of critical services in the event of a natural disaster, fire, act of terror, or other catastrophic event as outlined in the ELC Continuing Offsite Operations Plan ("COOP").

Access Control

Access to the ELC's systems shall be limited to those persons that need such access to perform their job or contractual duties. Procedures and protocols are to be in place to address and document the tasks that activate access to any production systems for ELC staff, its agents, its Contractors, its Vendors or other authorized persons and to deactivate/remove access to all production systems for outgoing or transferring ELC staff, its agents, its Contractors, its Vendors or other authorized persons as designated by the ELC that are in compliance with OEL's IT policy regarding personnel security. These include, but are not limited to, the following:

- Documentation for managing access criteria for information resources.
- The return of any office information resources (property or data).
- Procedures for unfriendly termination that include the prompt removal of system access.
- Audit trails shall be created and maintained to provide accountability for all access to confidential and exempt information and products.
- Audit trails for all changes to automated security or access. Examples include removal of access privileges, computer accounts and authentication tokens.

The ELC complies with requirements for deleting operational data from disposed equipment described in OEL's IT Security Policy.

Identification and Authentication

Access to ELC systems shall be granted to identified and authenticated users only.

Antivirus

This policy is in place so that the ELC, its agents, its Contractor, its Vendors or other authorized persons as designated by the ELC may verify that all computer systems are protected with antivirus and anti-malware software and that techniques are employed for avoiding viruses, malwares and other malicious programs to ELC systems.

Physical and Environmental Security

Automated information systems and facilities require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of ELC staff. Computer systems, facilities, confidential records, personally identifiable information ("PII"), protected personally identifiable information ("PPII") and disk storage areas shall be protected from theft, alteration, destruction, damage (i.e. fire, dust, misuse, water, etc.), power loss and other contaminants and unauthorized disruption of operation.

Change Control

All security changes made to any ELC systems shall be made in a controlled and coordinated fashion to preserve the confidentiality, integrity and availability of the system. No change to the ELC systems shall be made without the approval of the Chief Information Officer and the Chief Executive Officer.

Backup and Recovery

Recoverable backups shall be maintained for all critical systems at the ELC or by its contracted third party. Backups of critical information resources must be performed, tested and appropriately managed. Backups will be performed according to the following schedule:

- a. All critical data and system configurations must be backed up on at least a daily basis;
- b. Applications and licenses will be backed up whenever there are changes to them; and
- c. The backing up of non-critical data is at the discretion of the data owner.
- d. Backups will be stored off-site in a secure, environmentally-controlled location.

Patch Management and System Updates

The ELC systems are to be maintained with updated security patches or system updates.

Server Security

Servers shall be made secure before placing them into the ELC operational environment and security shall be maintained throughout their lifecycle. In the event the ELC uses a third-party server or cloud-based service for its ELC systems, the ELC shall ensure that the third party server or cloud-based service is secure before placing them into the ELC operational environment and that the third party who owns or is in control of the third party server or cloud-based service properly maintains security throughout their lifecycle of the contract or the state of Florida retention schedule, whichever is applicable.

Cloud Security

Cloud-based systems used to store, process, or transmit Coalition information must be approved by the IT Department. Cloud services must implement appropriate encryption, access controls, audit logging, backup capabilities, and security safeguards.

Mobile Computing

Security controls shall be implemented to mitigate the increase risks posed by the use of laptops and other mobile devices outside of the ELC main or satellite offices or ELC program sites. Those ELC employees are part of the ELC's telework program as set forth in the ELC's Telework Policy and Procedure shall be required to comply with this policy as applicable.

Network Security

Network devices and connectivity components shall be made secure before placing them into the ELC's operational informational technology environment, and security shall be maintained throughout their lifecycle.

Remote Access

Remote access shall mean any access to the office network through a network, device, or medium that is not controlled by the ELC (such as the Internet, public phone line, wireless carrier, or other external connectivity). Security controls shall be implemented to mitigate increased risks posed by allowing remote connectivity to ELC systems.

Electronic Mail

Electronic mail shall be protected from threats and vulnerabilities that can cause system damage, data compromise and business disruption.

Database Security

Securing information, so that it remains consistent, complete and accurate, is essential to the reputation, mission and critical business objectives of the ELC. Information shall remain consistent, complete and accurate.

Electronic Media Management

Electronic media shall be handled, stored and disposed of properly in order to protect the confidentiality of the ELC data, records, files and other information.

Password Management

Passwords are an important aspect of information security. The ELC shall protect access to its systems by ensuring that any passwords used for authentication are properly assigned and protected. The ELC staff shall also comply with requirements for passwords described in the user access management procedures.

Information Technology Asset Management

All information technology assets are tracked for inventory purposes by the Finance/Administration department.

Confidentiality Statement

The provisions of the Florida Public Records Act and other applicable state and federal laws will govern disclosure of any confidential information received by the state of Florida.

The ELC acknowledges each agency, organization or individual receiving confidential and exempt record in order to carry out official functions must protect all records, file data or other information. Those with access to data, records, files or other information other information that is confidential and exempt from disclosure in accordance with federal and Florida law ("Confidential Information") must not permit persons other than those authorized to receive the Confidential Information concerning a Client's personal identification.

ELC staff as well as any other authorized persons or entities as designated by the ELC shall ensure confidentiality and privacy regarding history, records and any discussions relating to the Clients who the ELC or its Contractor, Subcontractors, or Vendors may serve. The very fact that a Client is served by the ELC, its Contractors, its Vendors or other authorized persons or entities as designated by the ELC shall be kept private or confidential unless disclosure is made under for reasons relating to law enforcement, a court order, fulfillment of a statutory requirement, fulfillment of the ELC mission that does not violate applicable law, or upon signed release by the Client. Neither ELC staff or other authorized persons as designated by the ELC shall not disclose any information about a Client, including whether that Client is served by the ELC, its Contractor or its Vendors, or any other authorized person or entity as designated by the ELC to anyone outside of the ELC, without prior approval of the Chief Executive Officer or other persons authorized by the Chief Executive Officer, if the CEO is so authorized to make said disclosure pursuant to applicable federal and Florida law or in accordance with ELC policies, procedures and bylaws.

The ELC, including its employees, subcontractors, agents or any or other authorized persons or entity as designated by the ELC to whom the ELC authorizes to receive or access Confidential Information as stated herein, shall not store, or allow to be stored, any Confidential Information on any portable storage media (e.g. laptops, thumb drives, flash drives, hard drives, etc.) or peripheral device with the capacity to hold information without encryption software installed on devices meeting industry standards (i.e. National Institute of Standards and Technology).

The principle of confidentiality shall be maintained in all programs, functions and activities. ELC staff, its agents, its Contractors, its Vendors or any or other authorized persons or entity as designated by the ELC shall not discuss any Client of the ELC with any unauthorized third party at any time, whether on or off duty while employed or under contract with the ELC. Confidentiality shall be maintained regardless of separation or termination of employment or termination or expiration of any contract with the Contractor, Subcontractor, Vendor or other authorized person or entity as designated by the ELC.

Maintenance

1. The ELC, its Contractors, its Subcontractors, its Vendors and/or any or other authorized persons or entity as designated by the ELC who receive early learning records in order to carry out official functions must

protect the data and records in a manner that will not permit the personal identification of a Client by persons other than those authorized to receive the records;

2. The Contractors, Subcontractors, and/or Vendors of the ELC as well as any or other authorized persons or entity as designated by the ELC shall have documented procedures to maintain confidentiality of early childhood and other confidential records consistent with this policy if said parties handle Confidential Information on behalf of the ELC;

2.

Security Risk Assessments

The Coalition shall periodically conduct cybersecurity and information security risk assessments to identify threats, vulnerabilities, and control deficiencies.

Assessment results shall be reviewed by executive management and used to strengthen security controls and practices.

COMPLIANCE AND MONITORING

1. The ELC, its officers, its ELC staff, its interns, its Members, its agents, its Contractors, its Subcontractors, its Service Providers and its Vendors as well as any other authorized persons or entity as designated by the ELC shall comply with the applicable confidentiality provisions set forth in Florida Statutes as applicable, which includes, but is not limited to those statutes, codes and other regulation that concerns the records of children participating in School Readiness ("SR") and Voluntary Pre-Kindergarten Education (VPK) Programs and shall not release any information regarding any of the ELC Clients, except as specifically authorized by Florida statutes. Failure to abide by the applicable confidentiality requirements as set forth in those applicable Florida statutes may constitute a criminal offense.
2. Monitoring by the ELC will ensure that the ELC's Contractors, Subcontractors, Service Providers and Vendors are in compliance with the following:
 - All confidentiality provisions and the record retention requirements as set forth in Florida and federal statutes, where applicable.
 - All data security measures of the Health Insurance Portability and Accountability Act ("HIPAA").
 - All requirements for the protection and securing of trademarks, patents, and other proprietary information as set forth in Florida and federal statutes, where applicable.
 - Vendors, contractors, consultants, and service providers with access to Coalition information or systems must maintain reasonable cybersecurity controls. The Coalition may require review of cybersecurity policies, security assessments, cyber liability insurance, audit reports, or other documentation before granting access. Any security incident involving Coalition information shall be reported immediately. Shall not use or disclose any information concerning a Client for any purpose not in conformity with state and federal law or regulations except upon written consent of the Client when authorized by law.
 - Shall comply with the Computer-Related Crimes Act, Chapter 815, Florida Statutes and shall demonstrate due diligence in safeguarding the ELC's information resources by establishing policies and procedures for information systems security that contain criteria and standards as set forth in OEL's policies and procedures.

USER ACCOUNT MANAGEMENT PROCEDURES

It is the policy of the ELC to ensure that those electronic accounts used to perform or deliver ELC related-services and assigned to ELC staff or other authorized parties by the ELC's IT department ("user accounts") are standardized in order to minimize the potential exposure of the ELC, which may result from unauthorized user account access. This includes the loss, distribution or unauthorized access or use of sensitive or company confidential data, intellectual property, damage to public image, damage to critical ELC systems, and other unforeseen damages. As a result, the following procedures will be followed:

1. All ELC staff must read and sign the **Memorandum of Understanding ("MOU") and Data Security Agreement**, and hereby made a part of this policy and procedure, on an annual basis.
2. User accounts and passwords are the initial line of defense in network security. The Human Resource Manager must approve the creation/change of account(s) for ELC staff by completing the **System User Account Form** and by reference made part of this policy and procedure. The **System User Account Form** shall be submitted to the IT Department for processing by the HR Manager. ELC staff are granted the necessary privileges based on their account settings (fiscal, program operations and administration) to access files on the network server to accomplish day-to-day work. The ELC's IT department will approve the creation/change of account(s) for authorized persons other than ELC staff by completing the **System User Account Form**.
3. Computer network passwords and user names are provided to ELC staff to prevent unauthorized access to a computer. New users must change their password at their initial logon. Passwords are required to be at least eight (8) characters in length, and contain characters from three of the following four categories: English uppercase, English lowercase characters, Base 10 digits (0 through 9) and Non-alphabetic characters. Passwords to the ELC network are set to automatically expire every 60 days and prompt ELC users to automatically change/reset their passwords. Passwords cannot be reused for at least six (6) changes. ELC users should not reveal their password to anyone including other ELC staff. Multi-factor authentication shall be required whenever technically feasible. Password resets may be required following suspected compromise, security incidents, or elevated risk conditions. Password sharing is prohibited.
4. ELC staff and other authorized persons as designated by the ELC shall understand their responsibility for safeguarding user names and passwords, and immediately notify their supervisor and/or the ELC's IT Department if they suspect that a password or the system credential has been compromised.
5. All user accounts are automatically set to lockout after three (3) unsuccessful/invalid login attend. Lockout account can only be reset manually by the ELC's IT Department. This policy will help prevent attackers from guessing users' passwords and it decreases the likelihood of successful attacks on the networks.
6. All workstations/laptops are set to automatically lockout (screen saver mode) after twenty minutes of inactivity timeout. ELC staff and other authorized persons as designated by the ELC are recommended to log off from the workstation/laptop when leaving the work area. Workstations/laptops should not be shut down overnight.
7. When an employee is transferred or employment is terminated or the work performed or delivered by an authorized person as designated by the ELC is completed or terminated by the ELC, the user network account will be changed or deactivated immediately. The Human Resources Manager will notify the ELC's

IT department via email or written documentation (i.e. **System User Account Form**) on the day of transfers or termination of employment that require changes to his/her user account.

SECURITY MANAGEMENT/ACCESS CONTROL

The ELC is committed to protect and safeguard all data and electronic information systems from unauthorized use. All ELC staff and other authorized persons as designated by the ELC are assigned a user account and are granted the necessary privileges based on their account settings to access the network and perform their job function.

In order to protect and safeguard all data and electronic information systems from unauthorized use, the following standards/guidelines will be implemented by the ELC's IT Department:

1. Security measures are implemented by only granting specific access privileges to users required to perform their job duties based on the **System User Account Form** request.
2. Data folders are safeguard and can only be accessible based on access privileges
3. Regularly review records of system and security activity such as audit logs and access activity reports. ELC IT Department will perform desktop audit.
4. Regularly review VPN remote access audit log.
5. ELC's IT Department will maintain a listing of ELC staff and other authorized persons as designated by the ELC who have been granted access, and will periodically review access permissions granted.
6. ELC's IT Department will ensure that those granted access to data system have an approved Level II background screening and have received information security training in accordance with ELC protocols.
- 3.
7. Multi-factor authentication (MFA) shall be required for:
 - a. Email systems
 - b. Remote access
 - c. Cloud applications
 - d. Administrative accounts
 - e. Systems containing confidential information

SECURITY TRAINING AND AWARENESS

Security training and awareness is very crucial to the safeguarding of ELC information resources. Information security protocol and standards cannot be effective unless all ELC staff and other authorized persons are aware of the importance of data security, understand the ELC security procedures and protocols, and perform required practices. To make information security effective, standards and procedures must be known, understood, believed to be beneficial, and be appropriately and consistently practiced.

Effective information is achieved when it becomes part of everyone's thinking with regard to daily operations and assignments. In order to achieve effective information security and awareness, all ELC users must complete training on ELC data security policies and procedures. This will consist of the following training activities:

4. Data security training and awareness will be provided to all new ELC staff and other authorized persons as designated by the ELC by the ELC's IT Department covering this policy and procedure. Training to new ELC staff must be completed as soon as practical but less than 30 days of new employment. Training to authorized persons other than ELC staff must be completed within 30 days of approval for access to ELC systems.
5. All ELC users must complete an annual data security training program provided by the IT department to refresh their knowledge of data security. In addition, all ELC Staff and other authorized persons as designated by the ELC must annually complete the Florida's Department of Children and Families ("DCF") Online Security Awareness Training.
6. All ELC Staff and other authorized persons as designated by the ELC must sign an annual agreement that they understand the ELC data security policies and procedures within the ELC computing resources policy and that they will abide by them (**Information Security Training Acknowledgement Form**).

ELECTRONIC MAIL

For purposes of this policy, electronic mail shall mean point-to-point messages, postings to newsgroups and list serves and any electronic messaging involving computers, computer networks or ELC systems. Unencrypted transfer of confidential information by e-mail is strictly prohibited. The ELC complies with requirements for antivirus programs and other required protection programs and protocols as described in OEL's IT Security Policy.

Only electronic mail that is related to ELC business is acceptable for use with the ELC.

The examples below are considered inappropriate and unacceptable use of electronic mail. In general, electronic mail should not be used for the initiation or re-transmission of:

- Chain mail that misuses or disrupts resources (i.e. electronic mail sent repeatedly from user to user, with requests to send to others);
- Harassing or hate mail (i.e. any threatening or abusive electronic mail sent to individuals or organizations that violates ELC rules and regulations and this policy);
- Virus hoaxes;
- Spamming or electronic mail bombing attacks (i.e. international electronic mail transmissions that disrupt electronic mail service);
- Sending or forwarding junk mail (i.e. unsolicited electronic mail that is not related to ELC business and which is sent without a reasonable expectation that the recipient would welcome receiving it);
- Any actions that defraud another or misrepresent or fail to accurately identify the sender;
- Sending copies of documents in violation of copyright laws;
- Inclusion of the work of others into electronic mail communications in violation of copyright laws;

- Use of electronic mail to harass, intimidate or defame others or to interfere with the ability of others to conduct ELC business;
- Use of electronic mail systems for any purpose restricted or prohibited by law, statute, ordinance or regulations;
- “Spoofing,” (i.e. constructing an electronic mail communication so that it appears to be from someone else);
- “Snooping,” (i.e. obtaining access to the files or electronic mail of others for purpose of satisfying idle curiosity);
- Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmission without proper authorization;
- Electronic mail or communications that attempt to hide the identity of the sender, or represent the sender as someone else from another entity; and
- Any other electronic communication that violates this policy, ELC Employee Handbook, or any other law, statute, regulation or ordinance.
- Political or lobbying activities
- Personal business or commercial activities

DATA BACKUP

The backup and maintenance of data is critical to the viability and operations of ELC, and it is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis. This policy is designed to protect data and to ensure it is not lost and can be recovered in the event of a hardware failure, destruction of data, or disaster. The ELC complies with requirements for data backups described in OEL’s IT Security Policy.

To comply with this policy, the following standard procedure was put in place to ensure proper data backup:

Software:

Recognized industry approved software is used to backup all ELC data on a nightly basis. Software can be used to restore data in the case of an emergency.

Schedule:

An automatic full data backup is performed online daily and saved to a secure off-site location. A network attached storage device is also used to generate data backup locally. The ELC’s IT Department monitors the success of these backups on a daily basis and periodically reviews/updates to policy and processes for

changes in operations, identifies important data files, periodically performs testing and restore backup files, reviews backups and performs regular backups.

ANTIVIRUS

To assure continued uninterrupted service and to minimize the impact of computer viruses on ELC systems, all ELC servers, workstations, laptops, as well as any computers used for remote access to connect to the ELC network must have antivirus software installed and kept up to date. All disk drives, USB flash drives, thumb drives downloaded files, etc., must be scanned before using them on computers, laptops, and servers.

In order to protect the ELC systems from viruses, malware, spam or other internet attacks, the following steps/actions must be taking by all ELC staff or other authorized persons as designated by the ELC:

1. Never install software on ELC computers without permission from the IT Department.
2. Never download files from unknown or suspicious sources.
3. ELC staff should not remove or disable antivirus or other protection software from any ELC computers.
4. If a computer virus, malware or other malicious program is suspected to have infected ELC systems, immediately notify your supervisor and the ELC's IT Department.
5. ELC staff or other authorized persons as designated by the ELC are responsible for taking appropriate precautions to avoid introducing viruses, malware or other malicious programs into the ELC computing environment.
6. Antivirus software is set to update automatically as new virus definitions are made available by the ELC's vendor for said software.
7. ELC's IT Department is responsible for deploying antivirus agent to each ELC network computers from the server and to regularly monitor the ELC antivirus console installed on the server to verify that antivirus protects all computer systems:
 - a. Antivirus software applies to all servers, workstations, and remote access computers;
 - b. Every server or computer that contains OEL data or conducts and form or OEL business runs antivirus software;
 - c. Antivirus software protects data, scan documents, attachments, emails and internet sites before use by staff; Antivirus program scan portable media devices;
 - d. Documentation is maintained to verify the purchase and installation of antivirus software.

MOBILE COMPUTING

The use of laptop computers and mobile devices provide flexibility and enhanced communications that allow ELC staff or other authorized persons as designated by the ELC to be more productive. However, the use of these devices outside of the offices of the ELC poses risks to those devices and the information they contain. These devices may also present a hazard to the ELC data systems upon their return to the office (for example, by

spreading a virus that was obtained outside the office). These devices have the capability for direct connectivity to the internet or other networks outside of the ELC network which lack the protections afforded by ELC network firewalls and other perimeter protections. Therefore, additional security measures must be implemented to mitigate increased security risks presented by mobile computing. This procedure establishes procedures for mobile computing and applies to all laptops and other mobile computing devices that are used to store or process ELC data. Coalition-owned mobile devices shall be managed through an approved Mobile Device Management (MDM) platform. The Coalition reserves the right to remotely lock, locate, or wipe Coalition-owned devices that are lost, stolen, compromised, or no longer authorized.

To protect the ELC data systems from the security risks mobile devices present when used, the following standards/guidelines must be implemented by ELC staff or other authorized persons as designated by the ELC:

1. Laptops and other mobile computing devices must be inventoried by the Finance/Admin department and tracked by the IT department personnel.
2. Laptops must have antivirus installed with current updated definitions. The firewall must be enabled on the laptop computer.
3. Confidential information placed on mobile devices must be protected against unauthorized access and encrypted. Storage of Confidential Information on any mobile device is prohibited by the ELC.
4. Mobile computer users are responsible for backing up their data that is stored on the mobile computer on a regular basis.
5. ELC staff are responsible to take reasonable precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.
6. ELC staff and other authorized persons as designated by the ELC must immediately report their supervisor and/or IT department any loss, theft, tampering, unauthorized access, or damage of any mobile device.
7. All ELC staff or other authorized persons requesting the use of mobile devices owned by ELC must complete and sign an **Equipment Checkout Authorization Form**. Any ELC staff or other authorized persons as designated by the ELC assigned an ELC mobile device must also complete an **Employee Receipt of Property Form**. The Employee Receipt of Property Form will be kept by Human Resources Manager for the ELC.
8. ELC's IT Department is responsible for auditing the use of ELC mobile computing devices to ensure compliance with the procedures and guidelines set forth in this protocol.
9. Equipment checked out to ELC staff or other authorized persons as designated by the ELC must be utilized for ELC related business.

REMOTE COMPUTING

Remote access to Coalition information systems provides operational flexibility and supports the efficient delivery of services. However, remote connectivity increases the risk of unauthorized access, data interception, and

cybersecurity threats. Therefore, appropriate security controls must be implemented to protect Coalition information resources accessed from outside the Coalition's network environment. This protocol establishes requirements for all remote access connections to Coalition systems and information resources. The purpose of this protocol is to safeguard the confidentiality, integrity, and availability of Coalition information and to reduce the risk of harm to Coalition systems, operations, and data. Only Coalition-approved and managed devices may connect to Coalition systems containing confidential or sensitive information. Multi-factor authentication shall be required for remote access whenever technically feasible. Remote access activity may be logged, monitored, and audited to support security and compliance requirements.

The following security measures must be implemented to mitigate the increased security risks presented by remote computing:

1. All ELC staff by default will have account settings set to deny remote access. Only upon request will the account settings be changed to allow remote access. ELC staff or other authorized persons as designated by the ELC must read and sign a **Remote VPN Access Form**. Only upon the approval of the Remote Access VPN Request Form will the employee or other authorized persons as designated by the ELC be allowed to remote VPN by the ELC's IT department.
2. All remote connectivity must be authenticated. Confidential Information transferred over a remote access connection must be encrypted to protect it from unauthorized disclosure.
3. All data security policies for use in the ELC office environment must also be observed when using or connecting to ELC resources while outside the ELC office environment.
4. Confidential Information is not to be stored on any non-ELC computers. It is the responsibility of ELC staff to ensure that their access devices and remote connections are not used by unauthorized persons (including family members).
5. ELC remote users may not change operating system configurations, install new software, alter equipment or download software from systems outside of ELC network onto ELC remote access computers.
6. To prevent unauthorized users from accessing Confidential Information, ELC remote users must log out up after completing a remote session.
7. ELC remote users are responsible for complying with the procedures and guidelines set forth in this protocol; protecting their remote access credentials and devices from disclosure to, or use by, unauthorized persons; and immediately reporting any suspected unauthorized use of their remote access account or any damage to or loss of ELC computer hardware, software, or data that has been entrusted in their care.
8. The ELC's IT Department is responsible for auditing the use of remote access to ensure compliance with the procedures and guidelines set forth in this protocol. The ELC's IT department will regularly review the remote access audit log.
9. Personal home computers are prohibited from connecting to ELC network.

USE OF INTERNET/WORLDWIDE WEB

The internet/worldwide web (collectively the “Internet”), can be a valuable research tool and resource for ELC and its ELC staff. However, as with all electronic communications and services, the use of the internet is subject to abuse.

Subject to all policies and prohibitions contained herein, those contained in the ELC Employee Handbook, and as otherwise set forth under relevant laws, statutes, regulations and ordinances, ELC staff or other authorized persons as designated by the ELC may utilize the internet to conduct ELC business and for limited personal use. However, in utilizing the Internet, ELC staff or other authorized persons as designated by the ELC must remain cognizant that:

1. Any messages or information sent by an employee to one or more individuals via an electronic network (e.g., bulletin board, on-line service, or Internet) are statements identifiable and potentially attributable to ELC. While some users include personal “disclaimers” in electronic messages, it should be noted that there would still be a connection with ELC, and the statement might still be legally imputed to ELC. All communications sent by ELC staff via a network must comply with this and other ELC policies, and may not disclose any confidential or proprietary information.
2. Network services and internet sites can and do monitor access and usage and can identify at least which Early Learning Coalition of Broward County/entity (and often which specific individual) is accessing their services. Thus, accessing a particular bulletin board or website leaves ELC-identifiable electronic “tracks” even if the employee merely reviews or downloads the material and does not post any message.
3. As previously noted, ELC will allow limited use of electronic mail for personal reasons for ELC staff. Subject to the restrictions noted in this policy, ELC staff may also access the internet for personal reasons on a limited basis.

Screensavers

ELC staff may retain approved screensavers on the hard drives of their computer, subject to the provisions and restrictions of this policy.

Sensitive Information

ELC staff or other authorized persons as designated by the ELC must be cognizant that certain information about providers and individuals affected by our programs is confidential by law or is otherwise sensitive information. Information such as social security numbers, financial information or private information concerning children, must be guarded and protected by all ELC staff or other authorized persons as designated by the ELC.

Games/Purchasing Private Goods and Services

ELC staff may not use ELC systems to access, play games, contests, audio, video or any other forms of entertainment. Similarly, ELC staff or other authorized persons as designated by the ELC may not use the ELC systems to purchase personal goods and services over the Internet.

VIOLATIONS OF POLICY

Accidental Violation Of Policy

Any ELC staff or other authorized persons or entity as designated by the ELC who believes that he/she has inadvertently or accidentally violated the provisions of this policy must disclose the same in writing to their supervisor within one (1) business day of such violation.

Requirements of Managers and Supervisors

Managers and supervisors are responsible for ensuring policy compliance and for taking appropriate action when violations are identified.

Reporting Violations

ELC staff or other authorized persons as designated by the ELC must report any violations of this policy to Human Resources and in accordance with ELC policies and procedures. ELC may also refer suspected violations of applicable law to appropriate law enforcement agencies.

No Duty to Defend

ELC reserves the right not to defend any employee or other authorized persons or entity as designated by the ELC for any action brought by any person or entity for violation of any law, statute, regulation or ordinance committed by such employee or other authorized persons or entity using the ELC systems. In addition, ELC reserves the right to seek indemnification or subrogation from any employee or other authorized persons or entity as designated by the ELC in any action to which ELC is made a party based upon the employee's violation of any law, statute, regulation or ordinance.

APPLICABLE LAWS

The ELC will comply with all applicable federal and Florida laws governing data security, breach of security, reporting incidents and confidentiality.

In the event this policy and procedure, whether in whole or in part, creates an unallowable conflict with applicable federal or Florida statute, codes or rules or the Grant Agreement, the applicable federal or Florida statute, codes or rules and Grant Agreement will prevail.

EXHIBIT A - MEMORANDUM OF UNDERSTANDING - OEL

The Office of Early Learning and the local Early Learning Coalitions recognize that the full participation of the coalitions as a partner is critical to the success of the school readiness programs and the sharing of data between all parties is contemplated in the School Readiness Act. Thus, OEL hereby agrees to make available to the early learning coalitions and their agents, for the limited purpose of performing their public duties, school readiness programs information that includes, but is not limited to, data which is maintained in the Enhanced Field System ("EFS"), Statewide Reporting System ("SRS"), the Single Point of Entry/Unified Waiting List ("SPE/UWL") system,

SharePoint and any replacement systems providing the same school readiness data.

I. Designation of System Administrator and Security Officer

Each Early Learning Coalition will appoint a System Administrator and a Security Officer. Each Early Learning Coalition will notify the Information Systems Security Officer for OEL in writing who the designated System Administrator and Security Officer will be. OEL encourages each early learning coalition to designate separate individuals for each role.

The Early Learning Coalitions; their System Administrators, Security Officers, staffs, and employees; and the early learning coalitions' participating partners, contractors, subcontractors, any subsequent subcontractors, and their employees agree to maintain the confidentiality of school readiness data to include, but not be limited to, Social Security numbers, parent and child information, payments, childcare provider information, household demographic information, resource and referral information, and all related information pursuant to State and Federal regulations unless such information has been exempted from non-disclosure for business purposes in accordance with State or Federal law. Such information may be released if a lawful and proper authorization has been submitted by a participant of the program or a childcare provider.

The early learning coalitions will ensure that their System Administrator, Security Officers, staff, and employees; and the early learning coalitions' participating partners, contractors, subcontractors, any subsequent subcontractors, and their employees are sufficiently trained relative to non-disclosure and confidentiality regarding applicable school readiness programs. The early learning coalitions will assign access to the school readiness data systems only to early learning coalition and Office of Early Learning staff, contractors, subcontractors and subsequent subcontractor employees who have been properly trained by the early learning coalition regarding the confidentiality of school readiness records and who have completed and signed the "Data Security Agreement".

The early learning coalitions will require the System Administrator, Security Officer, staff, contractors, subcontractors, and any subsequent subcontractors and their employees who have access to confidential information to sign and comply with the "Data Security Agreement." The ELC will maintain these forms on file subject to inspection by the Office of Early Learning.

Early Learning Coalitions will advise their System Administrator, Security Officer, staff, contractors, subcontractors, and any subsequent subcontractor and their employees that they are not to make copies of confidential documents or to access, allow access to and/or use any confidential information for personal intent or any purpose other than in performance of their official duties.

II. Confidentiality and Public Access

All documents, papers, computer files, letters or other materials made or received in conjunction with the Agreement will be subject to the applicable legal requirements for maintaining confidentiality in conformance with Federal, State and local laws.

Public access to these records will be in accordance with Chapter 119 of the Florida Statutes and all other applicable laws or regulations.

Although the early learning coalitions' staff, contractors, subcontractors and their employees may obtain access to information that is otherwise confidential, that access does not alter the confidential nature of the information. It is incumbent upon the early learning coalitions; their System Administrators, Security Officers, staffs, and employees; and the early learning coalitions' participating partners, contractors, subcontractors, any subsequent subcontractors, and their employees to maintain confidentiality requirements.

Any requests for release of information covered under this Agreement by parties other than those specified in this

Agreement will be referred to the Office of Early Learning.

ITEM/MEETING	GOV271RB5 / Governance
DATE:	September 24, 2026
SUBJECT:	AI Policy
FOR ACTION:	Yes
RECOMMENDED ACTIONS:	Approve Proposed AI Policy Changes
FINANCIAL IMPACT:	None
AS RECOMMENDED BY	Staff
POLICY #	IT-POL-002
POLICY HISTORY	Gov May 1, 25; Board May 12, 2025
ELC STAFF LEAD	H. Cesar

Background Information:

The Board previously approved the Coalition's Artificial Intelligence (AI) Acceptable Use Policy to establish guidelines for the responsible and secure use of AI technologies in the workplace. Since its adoption, AI technologies and their use in business operations have continued to evolve, creating a need to periodically review and update the policy. Markups

Staff conducted a review of the existing policy and identified opportunities to strengthen governance, oversight, data protection, and employee guidance related to the use of AI tools. The proposed revisions are intended to provide clearer expectations for the use of AI technologies while supporting the Coalition's commitment to privacy, security, accuracy, accountability, and responsible innovation.

Current Status:

Staff completed a review of the Coalition's AI Acceptable Use Policy and are recommending several revisions to strengthen governance, oversight, and data protection requirements related to the use of AI technologies.

Key revisions include requiring written approval from the COO or Security Officer before AI tools may be used for Coalition business purposes. The revisions also prohibit the entry of confidential, exempt, sensitive, regulated, student, employee, financial, legal, procurement, or operational information into unapproved AI tools. In addition, the policy clarifies that AI-generated content may not be used as the sole basis for employment, compensation, disciplinary, legal, financial, procurement, regulatory, or other material organizational decisions without human review and approval.

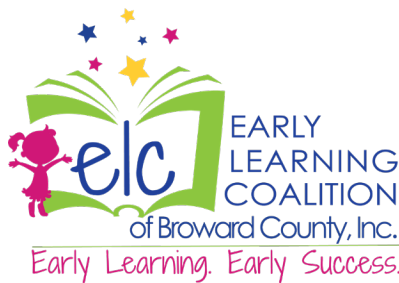
Additional revisions establish formal approval requirements for AI tools used for Coalition business purposes, expand the list of prohibited AI uses, require review and approval of AI systems that connect to Coalition data or business systems, and provide clearer guidance regarding the use of approved enterprise AI tools such as Microsoft Copilot. The revisions also reinforce employee responsibilities for reviewing, validating, and fact-checking AI-generated content before it is used or distributed. These updates are intended to strengthen safeguards around the use of AI technologies while protecting Coalition data, operations, and decision-making processes.

Recommended Action from Staff:

Approve Proposed AI Policy Changes

Supporting Documentation:

- Proposed Policy with marked changes
- Proposed Policy with no marked changes



ELC Artificial Intelligence (AI) Acceptable Use Policy

A. PURPOSE

This policy establishes guidelines for the responsible use of AI tools by ELC employees using company-issued equipment. AI and generative AI should enhance, not replace, human expertise.

B. ACCEPTABLE USE

ELC recognizes the benefits of AI in improving efficiency and productivity. However, AI also introduces risks such as privacy breaches, misuse, and unintended consequences. AI must be used responsibly, ethically, and in compliance with legal and organizational standards. This policy ensures that AI enhances operations while safeguarding data privacy, fairness, and transparency. AI-generated content must be proofread, edited, and fact-checked before use.

C. BACKGROUND

Generative AI refers to advanced machine learning models trained on large datasets to produce content based on user input. Examples include ChatGPT, Copilot, and DALL-E. These tools are rapidly evolving and should be used with caution to mitigate risks related to misinformation, bias, and data privacy concerns.

D. DEFINITIONS

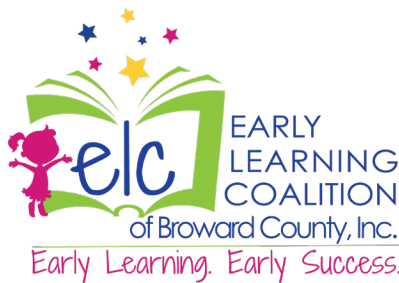
- **Artificial Intelligence (AI):** Machines performing tasks that require human intelligence.
- **Generative AI:** AI that generates text, images, or videos based on prompts.
- **Machine Learning:** AI that learns patterns from data to improve performance.
- **Algorithm:** A set of rules used for decision-making or problem-solving.
- **Prompt:** Input provided to an AI system to generate responses.

E. PRINCIPLES FOR USING GENERATIVE AI

1. Privacy

Data/information feeding the Generative AI tools are subject to public disclosure. This includes any text, photos, videos, or voice recordings you share with the AI. Be mindful that the AI output may consist of unexpected personal information from another user and ensure that any potential private information is removed before publishing.

Approved AI systems that provide enterprise-level security and privacy protections, such as Microsoft Copilot under ELC's Microsoft 365 environment, may be used for business purposes in accordance with ELC data handling requirements. Employees must not enter confidential, sensitive, regulated, or personally identifiable information into unapproved AI systems.



2. Accuracy

ELC maintains trust with our clients and partners by providing accurate information. Review and fact check all outputs you receive from a Generative AI. Users should consult trustworthy sources to confirm that the facts and details in the AI-generated content are accurate. Reliable sources include official ELC documents and peer-reviewed journals. Consult the IT Team for other trustworthy sources (e.g., newspapers, blogs, or datasets). AI systems may provide outdated, incomplete, inaccurate, or misleading information. Users must independently verify all factual statements, references, calculations, recommendations, and conclusions before relying upon or distributing AI-generated content. Keep in mind the tone and specific language in the AI output needs to reflect ELC communication styles. Generative AI is trained in a global context and may not use the vocabulary or tone consistent with the ELC and its values.

3. Proofreading and Fact-Checking

All AI-generated content must be proofread and validated for grammar, spelling, and accuracy.

4. Transparency

Clearly label AI-generated content and disclose AI usage when applicable.

5. Reducing Bias and Harm

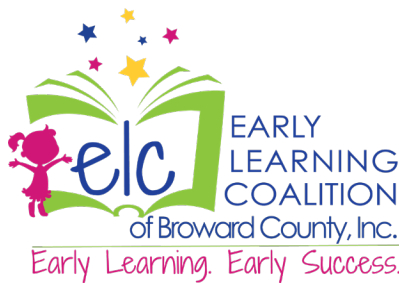
AI system responses are based on patterns and relationships learned from large datasets derived from existing human knowledge, which may contain errors and bias. Staff must ensure that AI-generated content does not discriminate against individuals based on legally protected characteristics. AI systems can reflect the cultural, economic, and social biases of the source materials used for training, and the algorithms used to parse and process that content can also be a source of bias. Employees should carefully review any content generated by AI to ensure that unintended or undesirable instances of bias, or even potentially offensive or harmful material, are changed or removed.

6. Accountability

The person using AI is accountable for the content it generates. Use Generative AI with a healthy dose of skepticism. It is always important to verify information provided by Generative AI.

7. Beneficial Use

Users should be open to responsibly incorporating Generative AI into their work where it can make services better, more just, and more efficient. For example, any AI generative tool can help users quickly go from an outline to a draft memorandum, enabling them to focus more on the analyses and findings that inform recommendations of the ELC's work and mission.



8. Prohibited Use

The use of AI-generated content in any work that violates ELC policies and procedures is strictly prohibited.

Generative AI may not be used as the sole basis for decisions involving employment, compensation, disciplinary action, legal determinations, financial commitments, regulatory compliance, procurement, or other decisions that could materially affect individuals or the organization. Human review and approval are required before any such decisions are made.

The use of artificial intelligence, including generative AI tools, chatbots, virtual assistants, automated content generators or similar technologies, is prohibited unless expressly reviewed, approved and authorized in writing by the COO or Security Officer.

Prohibited uses:

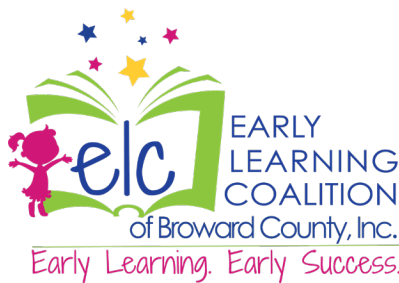
- Entering, uploading, copying, pasting, transmitting or otherwise providing confidential, exempt, sensitive, regulated, student, employee, financial, security, procurement, legal or operational information into any AI tool that has not been formally approved.
- Using AI tools to make or support final agency decisions, eligibility determinations, disciplinary actions, personnel decisions, student related determinations or other official actions without authorized human review and approval.
- Using personal accounts, personal devices, browser extensions, mobile applications or unauthorized third-party platforms to conduct Department business through AI tools.
- Using AI-generated content in official communications, reports, public-facing materials, procurement documents, legal documents, or decision-making records without appropriate validation, fact-checking, review, and approval.
- Using AI tools in a manner that violates federal and state law, Department policy, cybersecurity standards, privacy requirements, public records obligations, intellectual property rights or contractual restrictions.

9. AI as a Starting Point

AI-generated content should be viewed as a starting point, not the finished product. While AI can provide a valuable tool for generating content, it cannot replace the creativity and critical thinking skills of human writers and editors.

F. FUNDAMENTAL RULES

- Never submit confidential information to generative AI.
- Review, revise, and fact-check AI-generated content before use.



- Disclose AI-generated content where applicable.
- Stay updated with this policy as AI guidelines evolve.

G. COMPLIANCE

Generative AI usage may be subject to the Public Records Act. Any retained conversations relating to ELC's work may be subject to public records requests and must comply with the ELC's retention policies. This means any prompts, outputs, or other information used in relation to a Generative AI tool may be released publicly. Do not use prompts that may include information not meant for public release, including confidential or personal data.

If you choose to use Generative AI for ELC-related work, it is highly recommended that you utilize your ELC assigned Microsoft 365 account (MyEmailAddress@elcbroward.org) and use Microsoft Copilot as the Gen AI tool. This account should not be used for any personal purpose. **Employees remain responsible for reviewing, validating, and approving all AI-generated content before use.**

APPROVAL OF AI TOOLS

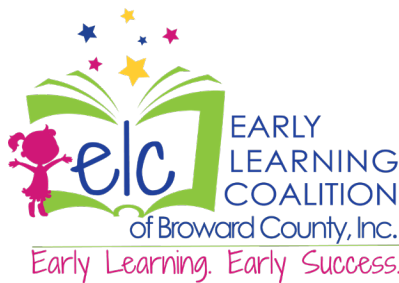
All software services, even if they are free or part of a pilot or proof-of-concept project, must be vetted, approved, and acquired by the ELC IT department before use to ensure the software receives all necessary reviews. This requirement applies to downloadable software, Software as a Service, web-based services, browser plug-ins, and smartphone apps. The use of generative AI technology incorporated into existing services and products, such as internet search engines, does not require permission, but these guidelines must be followed.

AI systems that connect to ELC data repositories, cloud services, email systems, document management systems, or business applications require review and approval by the Information Technology Department prior to implementation.

I. INTELLECTUAL PROPERTY

Content produced by generative AI systems may include copyrighted material. AI systems may be "trained" using data (text, images, etc.) sourced from the internet without regard for copyright or licensing terms. It is extremely difficult to determine what content was used to train an AI system and difficult to verify whether AI-generated content is wholly original or only a slight stylization of

existing copyrighted material. Nevertheless, employees must perform due diligence to ensure that no copyrighted material is published without proper attribution or obtaining proper rights.



For example, ELC employees could check the copyright of text-based content with plagiarism software and the copyright of image-based content with reverse Google searches, although neither of these approaches guarantees protection against copyright infringements. If users are uncertain if content violates copyright, they should either edit the content to be original or not use it.

J. ATTRIBUTION & ACCOUNTABILITY

Audiences should know when content was produced by AI as a whole or in part. If an employee uses AI-generated content in an official capacity, the content should be clearly labeled as having been produced using generative AI tools. Employees should also consider including information about how the material was reviewed and edited and by whom. This allows consumers of the content to understand its authorship and evaluate the content accordingly.

K. DATA PRIVACY

Employees must not submit sensitive, confidential, regulated, or personally identifiable data or data to a generative AI system. ELC recommends that Microsoft Copilot be used, as it provides the protected mode for the organization as part of our Microsoft 365 subscription.

Employees must not upload passwords, financial account numbers, Social Security numbers, health information, student records, personnel records, protected client information, or other regulated data into any AI system unless specifically authorized by ELC and protected by appropriate contractual and technical safeguards.

L. OWNERSHIP OF GENERATED CONTENT

In most cases, the user owns the content they input into a Generative AI service and the information they receive as an output. The user can use the content at their discretion, in accordance with ELC policy and any terms and conditions he/she has agreed to. However, many Generative AI companies still retain the right to use both the input and output content for their own commercial purposes.

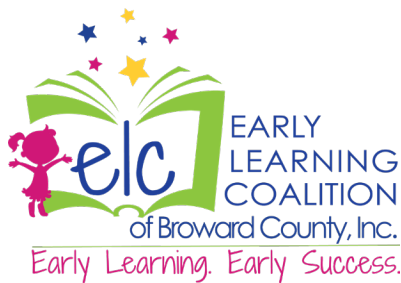
M. GUIDANCE ON USING GENERATIVE AI

Sample Use Cases

- Drafting memoranda or job descriptions.
- Developing presentation outlines and training materials.
- Summarizing lengthy documents.

Generating ideas for process improvements and operational efficiencies.

N. POLICY VIOLATIONS



- Non-compliance may result in disciplinary actions, including termination or legal consequences.

O. PRIVACY WAIVER

- ELC reserves the right to monitor employee use of AI and other digital tools.

P. ACKNOWLEDGMENT OF POLICY

By signing below, you acknowledge that you have read, understood, and agree to abide by ELC's AI Acceptable Use Policy.

Employee Name (Print): _____

Employee Signature: _____

Date: _____



ELC Artificial Intelligence (AI) Acceptable Use Policy

Draft

Pending Approval

Presented to

Governance on 9/24/26

Board on 10/05/26



ELC Artificial Intelligence (AI)

Acceptable Use Policy

A. PURPOSE

This policy establishes guidelines for the responsible use of AI tools by ELC employees using company-issued equipment. AI and generative AI should enhance, not replace, human expertise.

B. ACCEPTABLE USE

ELC recognizes the benefits of AI in improving efficiency and productivity. However, AI also introduces risks such as privacy breaches, misuse, and unintended consequences. AI must be used responsibly, ethically, and in compliance with legal and organizational standards. This policy ensures that AI enhances operations while safeguarding data privacy, fairness, and transparency. AI-generated content must be proofread, edited, and fact-checked before use.

C. BACKGROUND

Generative AI refers to advanced machine learning models trained on large datasets to produce content based on user input. Examples include ChatGPT, Copilot, and DALL-E. These tools are rapidly evolving and should be used with caution to mitigate risks related to misinformation, bias, and data privacy concerns.

D. DEFINITIONS

- **Artificial Intelligence (AI):** Machines performing tasks that require human intelligence.
- **Generative AI:** AI that generates text, images, or videos based on prompts.
- **Machine Learning:** AI that learns patterns from data to improve performance.
- **Algorithm:** A set of rules used for decision-making or problem-solving.
- **Prompt:** Input provided to an AI system to generate responses.

E. PRINCIPLES FOR USING GENERATIVE AI

1. Privacy

Data/information feeding the Generative AI tools are subject to public disclosure. This includes any text, photos, videos, or voice recordings you share with the AI. Be mindful that the AI output may consist of unexpected personal information from another user and ensure that any potential private information is removed before publishing.

Approved AI systems that provide enterprise-level security and privacy protections, such as Microsoft Copilot under ELC's Microsoft 365 environment, may be used for business purposes in accordance with ELC data handling requirements. Employees must not enter confidential, sensitive, regulated, or personally identifiable information into unapproved AI systems.



2. Accuracy

ELC maintains trust with our clients and partners by providing accurate information. Review and fact check all outputs you receive from a Generative AI. Users should consult trustworthy sources to confirm that the facts and details in the AI-generated content are accurate. Reliable sources include official ELC documents and peer-reviewed journals. Consult the IT Team for other trustworthy sources (e.g., newspapers, blogs, or datasets). AI systems may provide outdated, incomplete, inaccurate, or misleading information. Users must independently verify all factual statements, references, calculations, recommendations, and conclusions before relying upon or distributing AI-generated content. Keep in mind the tone and specific language in the AI output needs to reflect ELC communication styles. Generative AI is trained in a global context and may not use the vocabulary or tone consistent with the ELC and its values.

3. Proofreading and Fact-Checking

All AI-generated content must be proofread and validated for grammar, spelling, and accuracy.

4. Transparency

Clearly label AI-generated content and disclose AI usage when applicable.

5. Reducing Bias and Harm

AI system responses are based on patterns and relationships learned from large datasets derived from existing human knowledge, which may contain errors and bias. Staff must ensure that AI-generated content does not discriminate against individuals based on legally protected characteristics. AI systems can reflect the cultural, economic, and social biases of the source materials used for training, and the algorithms used to parse and process that content can also be a source of bias. Employees should carefully review any content generated by AI to ensure that unintended or undesirable instances of bias, or even potentially offensive or harmful material, are changed or removed.

6. Accountability

The person using AI is accountable for the content it generates. Use Generative AI with a healthy dose of skepticism. It is always important to verify information provided by Generative AI.

7. Beneficial Use

Users should be open to responsibly incorporating Generative AI into their work where it can make services better, more just, and more efficient. For example, any AI generative tool can help users quickly go from an outline to a draft memorandum, enabling them to focus more on the analyses and findings that inform recommendations of the ELC's work and mission.

8. Prohibited Use

The use of AI-generated content in any work that violates ELC policies and procedures is strictly prohibited.

Generative AI may not be used as the sole basis for decisions involving employment, compensation, disciplinary action, legal determinations, financial commitments, regulatory compliance, procurement, or other decisions



that could materially affect individuals or the organization. Human review and approval are required before any such decisions are made.

The use of artificial intelligence, including generative AI tools, chatbots, virtual assistants, automated content generators or similar technologies, is prohibited unless expressly reviewed, approved and authorized in writing by the COO or Security Officer.

Prohibited uses:

- Entering, uploading, copying, pasting, transmitting or otherwise providing confidential, exempt, sensitive, regulated, student, employee, financial, security, procurement, legal or operational information into any AI tool that has not been formally approved.
- Using AI tools to make or support final agency decisions, eligibility determinations, disciplinary actions, personnel decisions, student related determinations or other official actions without authorized human review and approval.
- Using personal accounts, personal devices, browser extensions, mobile applications or unauthorized third-party platforms to conduct Department business through AI tools.
- Using AI-generated content in official communications, reports, public-facing materials, procurement documents, legal documents, or decision-making records without appropriate validation, fact-checking, review, and approval.
- Using AI tools in a manner that violates federal and state law, Department policy, cybersecurity standards, privacy requirements, public records obligations, intellectual property rights or contractual restrictions.

9. AI as a Starting Point

AI-generated content should be viewed as a starting point, not the finished product. While AI can provide a valuable tool for generating content, it cannot replace the creativity and critical thinking skills of human writers and editors.

F. FUNDAMENTAL RULES

- Never submit confidential information to generative AI.
- Review, revise, and fact-check AI-generated content before use.
- Disclose AI-generated content where applicable.
- Stay updated with this policy as AI guidelines evolve.

G. COMPLIANCE

Generative AI usage may be subject to the Public Records Act. Any retained conversations relating to ELC's work may be subject to public records requests and must comply with the ELC's retention policies. This means any



prompts, outputs, or other information may be released publicly. Do not use meant for public release, including confidential or personal data.

used in relation to a Generative AI tool prompts that may include information not

If you choose to use Generative AI for ELC-related work, it is highly recommended that you utilize your ELC assigned Microsoft 365 account (MyEmailAddress@elcbroward.org) and use Microsoft Copilot as the Gen AI tool. This account should not be used for any personal purpose. **Employees remain responsible for reviewing, validating, and approving all AI-generated content before use.**

APPROVAL OF AI TOOLS

All software services, even if they are free or part of a pilot or proof-of-concept project, must be vetted, approved, and acquired by the ELC IT department before use to ensure the software receives all necessary reviews. This requirement applies to downloadable software, Software as a Service, web-based services, browser plug-ins, and smartphone apps. The use of generative AI technology incorporated into existing services and products, such as internet search engines, does not require permission, but these guidelines must be followed.

AI systems that connect to ELC data repositories, cloud services, email systems, document management systems, or business applications require review and approval by the Information Technology Department prior to implementation.

I. INTELLECTUAL PROPERTY

Content produced by generative AI systems may include copyrighted material. AI systems may be “trained” using data (text, images, etc.) sourced from the internet without regard for copyright or licensing terms. It is extremely difficult to determine what content was used to train an AI system and difficult to verify whether AI-generated content is wholly original or only a slight stylization of existing copyrighted material. Nevertheless, employees must perform due diligence to ensure that no copyrighted material is published without proper attribution or obtaining proper rights.

For example, ELC employees could check the copyright of text-based content with plagiarism software and the copyright of image-based content with reverse Google searches, although neither of these approaches guarantees protection against copyright infringements. If users are uncertain if content violates copyright, they should either edit the content to be original or not use it.

J. ATTRIBUTION & ACCOUNTABILITY

Audiences should know when content was produced by AI as a whole or in part. If an employee uses AI-generated content in an official capacity, the content should be clearly labeled as having been produced using generative AI tools. Employees should also consider including information about how the material was reviewed and edited and by whom. This allows consumers of the content to understand its authorship and evaluate the content accordingly.



K. DATA PRIVACY

Employees must not submit sensitive, confidential, regulated, or personally identifiable data or data to a generative AI system. ELC recommends that Microsoft Copilot be used, as it provides the protected mode for the organization as part of our Microsoft 365 subscription.

Employees must not upload passwords, financial account numbers, Social Security numbers, health information, student records, personnel records, protected client information, or other regulated data into any AI system unless specifically authorized by ELC and protected by appropriate contractual and technical safeguards.

L. OWNERSHIP OF GENERATED CONTENT

In most cases, the user owns the content they input into a Generative AI service and the information they receive as an output. The user can use the content at their discretion, in accordance with ELC policy and any terms and conditions he/she has agreed to. However, many Generative AI companies still retain the right to use both the input and output content for their own commercial purposes.

M. GUIDANCE ON USING GENERATIVE AI

Sample Use Cases

- Drafting memoranda or job descriptions.
- Developing presentation outlines and training materials.
- Summarizing lengthy documents.

Generating ideas for process improvements and operational efficiencies.

N. POLICY VIOLATIONS

- Non-compliance may result in disciplinary actions, including termination or legal consequences.

O. PRIVACY WAIVER

- ELC reserves the right to monitor employee use of AI and other digital tools.

P. ACKNOWLEDGMENT OF POLICY

By signing below, you acknowledge that you have read, understood, and agree to abide by ELC's AI Acceptable Use Policy.

Employee Name (Print): _____

Employee Signature: _____

Date: _____

ITEM #/MEETING:	GOV271RB6/ Governance
DATE:	September 24, 2026
SUBJECT:	Remote and Hybrid Work Policy
FOR ACTION:	Yes
RECOMMENDED ACTION:	Approve proposed Remote and Hybrid Work Policy
FINANCIAL IMPACT:	None
AS RECOMMENDED BY	Staff
Policy #	HR-POL-001
ELC STAFF LEAD	Hubert Cesar/Michelle Perez

Background Information:

The ELC has operated with a predominantly remote and hybrid workforce since 2020 and uses an Employee Telework Agreement to document individual remote work arrangements. During this period, the Coalition has continued to evaluate its workforce needs, operational requirements, technology capabilities, and employee feedback to ensure that remote and hybrid work arrangements support both organizational effectiveness and employee productivity. As remote and hybrid work has become a long-term component of the Coalition's operating model, staff conducted a review of the existing policy and related practices to ensure they continue to reflect current business operations and management expectations.

The proposed policy updates clarify eligibility requirements, employee and supervisor responsibilities, performance expectations, work location requirements, technology and equipment standards, and other administrative provisions associated with remote and hybrid work arrangements. The revisions are intended to provide greater consistency in the administration of remote work while maintaining flexibility to support business needs, continuity of operations, employee engagement, and service delivery.

Current Status

The proposed policy provides a common framework for approving and administering remote and hybrid work while allowing arrangements to reflect position requirements and operational needs. It brings eligibility, availability, work location, performance, and information-security expectations into one reference for employees and management.

The policy establishes remote and hybrid work as discretionary arrangements requiring management and Human Resources approval and a signed Employee Telework Agreement. Employees generally must successfully complete their 90-day introductory period before becoming eligible, subject to approved exceptions and applicable accommodation requirements. Employees must maintain their approved schedule, remain accessible, meet established performance standards, and report on-site when directed, subject to approved leave, accommodations, or other approved exceptions.

Employees must maintain their primary residence and approved remote-work location in Florida. The policy permits work outside Florida during authorized ELC business travel within the United States. Work during personal travel outside Florida requires a reasonable and necessary business need and advance written approval from the supervisor, Human Resources, and executive management following review of location, duration, payroll, legal, and security considerations. These personal-travel exceptions are limited to the shortest necessary period, not exceeding ten consecutive workdays. Work and access to ELC systems or information from outside the United States are prohibited.

The policy applies ELC's timekeeping, overtime, equipment, confidentiality, cybersecurity, public-records, and safety requirements to remote work. It addresses secure internet access, accurate reporting of all time worked by nonexempt employees, work interruptions, injuries, monitoring, and travel expenses. These provisions reinforce employee responsibilities and the protection of ELC information and property.

ELC may modify or end arrangements based on operational or other business considerations, subject to applicable law. Individualized accommodations remain available through ELC's accommodation process, including modification of

ordinary eligibility requirements when required. The policy supports accountability and consistent decisions while preserving operational flexibility.

Recommended Action from Staff:

Approve proposed Remote and Hybrid Work Policy.

Supporting Documents

Draft Remote and Hybrid Work Policy



Remote and Hybrid Work Policy

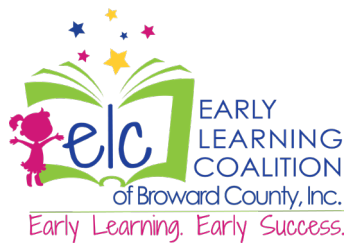
Draft

Pending Approval

Presented to

Governance on 9/24/26

Board on 10/05/26



Remote and Hybrid Work Policy

ELC recognizes that remote and hybrid work arrangements may support organizational effectiveness, employee productivity, and business continuity when consistent with the requirements of the position and ELC's operational needs. This policy establishes the conditions under which an employee may be authorized to perform work from an approved residence or other approved remote location.

For purposes of this policy, "remote work" or "telework" means performing assigned ELC work from an approved location other than an ELC office or other assigned worksite. "Hybrid work" means an approved schedule that combines remote work with work at an ELC office or other assigned worksite. Remote and hybrid work are different from off-site assignments at provider, community, partner, or other ELC-approved business locations.

Eligibility and Approval

Remote and hybrid work are discretionary workplace arrangements and are not employee entitlements, guaranteed benefits, or terms of employment. ELC determines which positions and employees are eligible based on the position's duties, operational and staffing needs, required in-person interaction, performance and attendance, supervisory requirements, information-security considerations, access to confidential records, available technology, and other relevant business factors.

Employees generally must successfully complete their 90-day introductory period before becoming eligible for a remote or hybrid work arrangement, unless ELC approves an exception or a different arrangement is provided as a reasonable accommodation or otherwise required by applicable law.

Approval of a remote or hybrid work arrangement requires authorization from the employee's management and Human Resources. Before beginning remote work, the employee must sign an Employee Telework Agreement identifying the approved work location and any employee-specific schedule, equipment, communication, or performance requirements. An employee may not begin working remotely merely because the employee has requested or discussed such an arrangement.

ELC may approve different remote or hybrid arrangements for different positions or employees based on legitimate operational considerations. Approval of one arrangement does not require ELC to approve the same arrangement for another position or employee.

Approved Work Location

Employees may perform remote work only from the location identified in their Employee Telework Agreement. Employees participating in a remote or hybrid arrangement must maintain their primary residence and approved remote-work location within the State of Florida. A temporary exception may not be used to establish or maintain a residence outside Florida.

Working outside Florida is prohibited unless the employee is traveling on authorized ELC business or ELC determines that a reasonable and necessary business need requires the employee to work during personal travel. Employee convenience, a desire to extend personal travel, avoid using leave, or remain available for routine work does not constitute a business need.

Any exception for personal travel must be approved in writing in advance by the employee's supervisor, Human Resources, and executive management. Approval will be considered only after evaluating the business need, location, duration, state and local payroll requirements, legal and regulatory risks, and information-security concerns. Any approval will be limited to the shortest period necessary and may not exceed ten (10) consecutive workdays.



Approval is discretionary, may be denied or revoked, and does not create an entitlement or precedent for future requests.

Employees are prohibited from performing work or accessing ELC systems, email, records, or information while outside the United States.

Employees must promptly notify Human Resources and their supervisor of any proposed change to their approved work location. A change of residence does not automatically transfer approval to the new location.

The approved remote workspace must provide sufficient privacy, security, internet connectivity, and freedom from disruptions to allow the employee to perform assigned duties safely, effectively, and confidentially. Employees are responsible for maintaining reliable internet service and other utilities necessary to perform assigned duties. Service interruptions do not relieve employees of their obligation to perform work and may require the employee to report to an ELC office or other management-approved work location.

On-Site Attendance

Remote and hybrid employees must maintain the ability to report to an ELC office or other designated worksite when directed. ELC may require on-site attendance for meetings, training, orientation, supervision, operational coverage, technology support, performance concerns, emergencies, or other business needs.

Employees must attend required on-site activities even when they fall on a day ordinarily scheduled for remote work. ELC will provide reasonable notice when practicable, but circumstances may require immediate or short notice on-site attendance.

A remote or hybrid schedule does not change an employee's assigned office, official headquarters, job duties, reporting relationship, or obligation to travel unless ELC expressly states otherwise in writing.

An employee must report to an ELC office or other designated worksite at the date and time directed by the employee's supervisor or management, even when the employee was scheduled to work remotely. An employee's remote-work schedule, commuting distance, transportation arrangements, dependent-care responsibilities, or personal plans do not excuse the employee from this requirement. Failure or refusal to report as directed, absent approved leave, a reasonable accommodation, or another management-approved exception, may result in modification or termination of the remote-work arrangement and corrective action, up to and including termination of employment.

Work Schedule, Availability, and Performance

Remote and hybrid employees must work their approved schedule and remain accessible, responsive, and actively engaged in ELC business during scheduled working hours. Employees are expected to respond promptly to telephone calls, electronic communications, meeting invitations, and work assignments and to maintain the same productivity, performance, conduct, attendance, and service standards that apply when working on-site.

Employees must promptly notify their supervisor of any power outage, internet disruption, weather event, emergency, or other circumstance that interfere with their ability to perform assigned duties. Depending on

operational needs, employees may be directed to report to an ELC office or other designated location, utilize available leave, or follow ELC emergency procedures.

Employees may not change their work schedule, work location, or remote-work days without prior approval. Remote work may not be used in place of vacation, sick leave, personal leave, or another applicable form of leave when the employee is unable to work.



Remote work is not intended to replace appropriate childcare, dependent care, or other caregiving arrangements. Employees are responsible for ensuring that dependents are adequately supervised and that personal responsibilities do not interfere with their ability to perform job duties, maintain confidentiality, participate in meetings, or remain available during scheduled working hours. Temporary schedule modifications require management approval.

Employees must participate professionally in virtual meetings. When requested and appropriate for the meeting, employees are expected to appear on camera, maintain professional attire and conduct, and use an ELC-approved or business-appropriate background, subject to an approved exception or reasonable accommodation.

Employees may not conduct in-person meetings with families, providers, vendors, members of the public, or other ELC business contacts at their residence unless expressly authorized by ELC.

Timekeeping and Overtime

ELC's Timekeeping Procedures and Overtime policies apply equally to remote and hybrid employees. Nonexempt employees must accurately record all time worked while working remotely and may not work outside their approved schedule, during an unpaid meal period, or beyond their scheduled hours without prior approval. All time worked must be reported, regardless of whether it was authorized. Failure to obtain required approval may result in corrective action or modification or termination of the remote-work arrangement.

Equipment, Supplies, and Expenses

ELC's Use of ELC Equipment/Materials and Business Expense Reimbursement policies, together with the Employee Telework Agreement, apply to all remote and hybrid work arrangements. ELC will determine the equipment, software, supplies, and system access necessary for each arrangement.

All ELC-issued equipment, software, records, documents, files, and data remain the property of ELC. Employees must safeguard ELC property and return all such property immediately upon request or upon termination of employment, unless otherwise directed by ELC.

Confidentiality, Cybersecurity, and Public Records

ELC's Confidentiality, Information Access and Electronic Communications and Confidentiality and Intellectual Property Rights policies apply equally when employees work remotely or under a hybrid arrangement. Employees must also comply with ELC's applicable information-security, cybersecurity, records-retention, and public-records procedures and the requirements of the DEL Grant Agreement.

Employees may not access, transmit, store, or conduct ELC business using open public Wi-Fi networks or other unsecured internet connections. Remote work must be performed using a secure private internet connection that complies with ELC's information-security requirements. Employees must follow all ELC cybersecurity procedures and may use only ELC-approved methods to access ELC systems, records, and data.

Workplace Safety and Injuries

Employees must maintain a designated remote workspace that is safe, orderly, and free from recognized hazards. ELC's safety expectations apply while employees are working remotely.

An employee who sustains an injury while performing assigned work at the approved remote location must immediately, or as soon as practicable, notify the employee's supervisor and Human Resources and comply with ELC's Work-Related Injuries Policy. Workers' compensation coverage will be determined under applicable law based on the circumstances of the injury.



Employees may not invite or permit ELC business contacts to enter their residence for ELC business unless expressly authorized.

Monitoring and Privacy

ELC's Workplace Monitoring Policy applies to employees working remotely or under hybrid arrangements. ELC may use appropriate technological means to verify that an employee is working from the approved location. This policy does not authorize access to an employee's personal devices, personal accounts, or areas of the employee's residence unrelated to ELC business, except as authorized by the employee or permitted by applicable law.

Travel and Mileage

Remote and hybrid employees must follow ELC's Business/Travel Expenses and Business Expense Reimbursement policies. Travel between an employee's home and ELC's main office is considered a commute and is not eligible for mileage reimbursement. Compensation for travel time, when applicable, will be determined in accordance with ELC's Travel Time for Non-Exempt Employees policy and applicable law.

Modification or Termination of Arrangement

ELC may modify, suspend, or terminate a remote or hybrid work arrangement at any time based on operational requirements, staffing, performance, attendance, conduct, technology, information security, funding requirements, or other business considerations, subject to applicable law. When practicable, ELC will provide reasonable notice.

An employee may request termination or modification of the arrangement through the employee's supervisor and Human Resources. Modification or termination of a remote-work arrangement does not, by itself, constitute disciplinary action.

Failure to comply with this policy, the Employee Telework Agreement, or another applicable ELC policy may result in modification or termination of the arrangement and corrective action, up to and including termination of employment.

Reasonable Accommodations

This policy does not limit ELC's obligations under the ADA, PWFA, or other applicable laws. Telework may be considered as reasonable accommodation through ELC's established accommodation process. ELC may waive or modify ordinary eligibility requirements when required as part of an individualized accommodation determination.