



EARLY LEARNING COALITION
OF POLK COUNTY
Heart of Education

Polk County School Readiness Coalition, Inc. dba Early Learning Coalition of Polk County

Request for Proposal for

DEDICATED INTERNET

ELCPOLK-FY2025-03

Date Issued: October 6, 2025

Due Date/Time: October 16, 2025 3:00p.m.

Inquiries and proposals should be directed in writing to:

Erica Clark
Procurement Specialist
contractmanager@elcpolk.org

Table of Contents

Section I – Introduction	Page
Introduction	3
Background	3
Statement of Purpose	4
Prohibition of Lobbying	4
Conflict of Interest	4
Public Information	4
Right to Reject Proposals and Waive Informalities	4
Clarification/Interpretation/Additional Information	4
Addendum	5
 Section II - Scope of Services	
Scope of Work	6
Time Requirements	6
Contract Period	6
Contract Value	6
Agreement	6
 Section III – Selection Method and Instructions	
Interest	7
Receipt of Submittals	7
Submittals List	7
Anticipated Schedule of Events	7
Evaluation Process	8
Evaluation Criteria	8
 Section IV – Terms, Conditions, and Other Requirements	
Federal and State Tax	9
Legal Requirements	9
Trade Secret and Confidential Materials	9
Monthly Invoicing and Payment	10
Option to Request Price Adjustment	10
Primary Point of Contact	10
Replacement of Personnel	10
Insurance	11
Termination	12
Contractor Indemnification	13
Subcontracting	14
Gratuities	14
Force Majeure	14
Effect of Prime Change	15
 Section V – Pricing Form and Specifications	16
 Attachments A-I	18

SECTION I – INTRODUCTION

1.1 Introduction

The Early Learning Coalition of Polk County (the Coalition) invites companies to submit proposals for Dedicated Internet as outlined in the Scope of Services to the Early Learning Coalition of Polk County located in Polk County, Florida. In order to be considered, proposal submissions must be received by 3:00 P.M. Eastern Standard Time on October 16, 2025.

1.2 Background

In 1999, the Florida Legislature passed the School Readiness Act. The Act created the Florida Partnership for School Readiness. In addition, the Act called for the creation of local school readiness coalitions whose goals were to improve the readiness of children when they enter school.

With specific membership designated by Florida Statutes, 57 school readiness coalitions were formed throughout the state covering all 67 counties.

In 2001, the Florida Partnership for School Readiness was transferred from the Executive Office of the Governor to the Agency for Workforce Innovation for administrative purposes. The funds for the Pre-Kindergarten, subsidized Child Care, Even Start, First Start, Migrant Pre-Kindergarten, and other programs were managed by the Agency for Workforce Innovation and distributed through the local coalition.

In early 2005, the State passed Voluntary Pre-Kindergarten (VPK) legislation, which placed local responsibility for the VPK program with the local school readiness coalitions. The coalitions have been renamed “Early Learning Coalitions” to reflect their greater role in meeting the early care and education needs of children and their families. To date, through the merging of Coalitions, there are now 30 Early Learning Coalitions throughout the state. Coalitions now fall under the direction and funding of the Division of Early Learning (DEL), a part of the Florida Department of Education.

The Coalition is charged with assessing the early care and education resources available in our community and developing local plans to address identified needs of children and their families. The Early Learning Coalition of Polk County plans, funds and administers a system of services designed to help ensure that children are ready for school when they enter kindergarten. In addition, the Coalition helps give parents support services to enable them to be stable and strong.

The Coalition’s budget for School Readiness and VPK combined is over \$40 million. We normally have between 300 and 400 active providers. This budget is funded by a mix of federal, state and local grants. The Coalition is charged with using this funding effectively and efficiently to achieve program goals.

1.3 Statement of Purpose

The objective of this Request for Proposal (“RFP”) is to procure dedicated internet access with a single service provider.

1.4 Prohibition of Lobbying

Any company or lobbyist, paid or unpaid, for a company is prohibited from having any private communication concerning the procurement process or any response to the procurement process with any Coalition Board Member, the Chief Executive Officer, or any employee of the Coalition after the issuance of this RFP and until completion of the contract award. A proposal from any organization will be disqualified when the company (or a lobbyist, paid or unpaid, for the company) violates this condition of the procurement process.

1.5 Conflict of Interest

All companies must disclose in their Letter of Certification the name of any officer, director or agent who is also a Coalition employee. All companies must disclose the name of any Coalition employee who owns, directly or indirectly, any interest in the company’s business or any of its branches. All companies must disclose any business relationships or family relations with any officer, board member, subcontractor, or employee of the Coalition.

1.6 Public Information

All submitted proposals and included or attached information shall become public record upon their delivery to the Coalition in accordance with Chapter 119, Florida Statutes. The contact person with respect to any or all aspects of this RFP is Erica Clark, Procurement, and she can be reached via e-mail at contractmanager@elcpolk.org

1.7 Right to reject Proposals and Waive Non-Material Irregularities

The Coalition reserves the right to accept or reject any or all proposals, waive any irregularities and technicalities contained therein, and may, at its sole discretion request a clarification of other information to evaluate any or all proposals. Contractors may be required to submit evidence of qualifications or any other information as the Coalition may deem necessary.

1.8 Clarification/Interpretation/Additional Information

Written questions concerning interpretation, clarification or additional information will be accepted via email. All questions must be received by the Procurement Department no later than the date and time as shown in the Anticipated Schedule of Events section. Telephone inquiries will not be accepted, nor will answers be provided by telephone. It is the sole responsibility of the proposer at its own risk to ensure that written questions will be received by the deadline indicated. If warranted, the Coalition will post the responses (as an addendum) to the same website where this solicitation is posted.

1.9 Addendum

The issuance of a written addendum is the only official method by which interpretation, clarification or additional information can be given. If it becomes necessary to revise or amend any part of this document, an addendum will be posted to the same website where this solicitation is posted. The Coalition may modify the Request for Proposal by issuance of a written addendum. Addenda shall be numbered consecutively.

SECTION II – SCOPE OF SERVICES

2.1 Scope of Work

The Early Learning Coalition of Polk County is requesting proposals for **installing dedicated fiber internet with a speed of 200 Mbps (or equivalent) inclusive of 5 static IP addresses for each location**. Locations of services include two properties: 1) Lakeland, FL office located at 115 S. Missouri Ave, Suite 201 and Suite 501. 2) Winter Haven, FL office located at 203 Avenue A. NW, Suite 101.

Proposals must include, but not limited to, the following:

Service Level Agreement-The respondent will provide a proposed service level agreement (SLA).

Service Level Guarantees-The respondent will provide a proposed service level guarantee along with a proposed credit, inclusive of a proposed procedure for requesting credits.

Reports-The respondent will provide available reports such as, but not limited to, incident reports.

Historical uptime-If available, uptime statistics for your proposed service in the geographic area.

The services will be rendered in a manner deemed satisfactory to the Coalition as determined by periodic monitoring and the review of required reports. Any modifications to the Scope of Services shall not be effective until approved in writing by both parties.

2.2 Time Requirements

All services and materials described under the Scope of Work must be in place by January 1, 2026.

2.3 Contract Period

The effective period for the services will be January 1, 2026-December 31, 2029. The initial term of this contract will be for a 3-year period. With the option to renew in two 1-year terms if agreed upon in writing by both parties.

2.4 Contract Value

The 3-year contract value is estimated between \$35,000-\$70,000 based on historical values. It is anticipated that one vendor will be selected for award.

2.5 Agreement

A professional services agreement will be negotiated for any work to be performed as a result of this RFP. The RFP, the proposal, and the resulting agreement will constitute the complete agreement between the company and the Coalition. This RFP alone, is in no way an agreement, obligation, or contract and in no way is the Coalition responsible for the cost of preparing the submittal packet. One copy of the submittal will be retained for official files and becomes a public record.

SECTION III – SELECTION METHOD AND INSTRUCTIONS

3.1 Interest

Companies who intend to respond to this RFP are requested to notify the Coalition by sending an email to contractmanager@elcpolk.org with the RFP number and name in the subject line no later than October 13, 2025. Please include the name, address, telephone, and email address of the company (firm) and contact person.

3.2 Receipt of Submittals

It is the sole responsibility of the vendor to ensure that their proposal is submitted no later than the time and date indicated in the RFP or as amended in the form of an addendum issued by the Procurement Department. The vendor is responsible for allowing adequate time. Submittals sent by facsimile, telephone, or any other means not specified herein will not be accepted. **Submittals in hard form will be accepted by mail or other means of delivery to: ELC 115 S. Missouri Ave 2nd Floor Suite 201 Attn: Erica Clark, Lakeland, FL 33815. Submittals will also be accepted via email to contractmanager@elcpolk.org.** Acceptable file formats for upload are Microsoft Excel (.xls or .xlsx), .pdf or .ZIP file formats. Printing must be enabled on all files submitted.

3.3 Submittals List

To help ensure that you include all the submittals necessary to complete a thorough evaluation of your packet, submittals should be provided according to the structure outlined here.

Tab	Description of Submittal	Page No.
Tab 1	All Signed Attachments A-H Attachment I (If applicable)	18-55
Tab 2	Filled in Pricing Form and Specifications	16-17
Tab 3	Vendor Proposal inclusive of Defined SOW and Service Level Agreement	6 (for guideline of requested Scope)

3.4 Anticipated Schedule of Events (Subject to change as conditions may dictate)

Activity	Date
Release of Request for Proposals	October 6, 2025
Deadline for Receipt of emailed (contractmanager@elcpolk.org) Questions - 4:00p.m.(ET)	October 8, 2025
Interest-email of intention to respond to RFP	October 13, 2025
Deadline for Answers to Questions (on or about)	October 14, 2025
Deadline for receipt of Proposals- 3:00 p.m.(ET)	October 16, 2025
Evaluation Committee Meeting to Review Responses (115 S. Missouri Ave Lakeland, 5 th floor, 9:00a.m.)	October 17, 2025
Posting of Award Recommendation (on or about)	October 21, 2025
Approval of Award recommendation (on or about)	October 24, 2025
Contract Start	January 1, 2026

3.5 Evaluation Process

The Vendor Selection Committee, consisting of Board Members and/or Coalition staff, will evaluate the proposals and prepare recommendations to the Chief Executive Officer and/or the Coalition Board of Directors. All submittals received will be reviewed in accordance with the criteria listed in this RFP. The Committee may ask additional questions to clarify the submitted proposal(s).

The Chief Executive Officer and/or the Coalition Board of Directors shall make the final decision. Once the selection has been made, contract negotiations will begin. If a contract agreement cannot be reached with the most successful company, negotiations with that company will be formally terminated. The Coalition would then negotiate with the next most successful company until an agreement is reached. The Coalition may choose to modify the choice of a selected company if the Coalition determines that such a change is in its best interest.

The Coalition reserves the right to reject any and all proposals submitted. The Coalition further reserves the right to inspect the facilities, organization, and review evidence of the financial condition of a company to assess their ability to perform the contract before awarding a contract.

3.6 Evaluation Criteria

The Evaluation Committee shall score and rank responsive proposals. The evaluation factors will be limited to the criteria listed in the table below:

Evaluation Criteria	Point Value
Required Attachments (Tab 1)	PASS/FAIL
Pricing (Tab 2)	20
Product/Specifications (Tab 2)	20
Proposal-SOW (Tab 3)	20
Proposal-Service Level (Tab 3)	40
TOTAL POINTS AVAILABLE	100

SECTION IV – TERMS, CONDITIONS AND OTHER REQUIREMENTS

4.1 Federal and State Tax

The Coalition is exempt from federal taxes; in addition, the Coalition is exempt from State and County tangible personal property taxes, sales taxes, and intangible taxes. The Coalition's Chief Executive Officer will sign an exemption certificate submitted by the successful company. The company doing business with the Coalition will not be exempted from paying sales tax to their suppliers for materials to fulfill contractual obligations with the Coalition, in addition, the successful company will not be authorized to use the Coalition's tax exemption number in securing such materials.

4.2 Legal Requirements

It shall be the responsibility of the provider to be knowledgeable of all federal, state, county and local laws, ordinances, rules and regulations that in any manner effect the items covered herein. Lack of knowledge by the company will in no way be a cause for relief from responsibility.

Companies doing business with the Coalition will be required to attest to compliance with the following federal and state rules and regulations:

- Equal Employment Opportunity (EO 11246 as amended by EO 11375 and supplemented by regulation 41 CFR part 60)
- Copeland "Anti-Kickback" Act (18 USC 874 and 40 USA 276c)
- Contract Work Hours and Safety Standards Act (40 USC 327-333)
- Rights to Inventions Made Under a Contract or Agreement (37 CFR part 401)
- Clean Air Act (42 USC 7401 et seq) and Federal Water Pollution Control Act (33 USC 1251 et seq), as amended
- Debarment and Suspension (EO 12549 and EO 12689)
- Employment Eligibility Verification (E-Verify) (F.S. 448.095)
- Discriminatory Vendor List (F.S. 287.134)

4.3 Trade Secret and Confidential Materials

If the application includes material which is deemed a trade secret (as defined by Section 812.081, FS) or other confidential material exempt from the provisions of Chapter 119, FS, which the company does not wish to become public record, the following statement should be included in the application:

"Trade Secrets as defined by Section 812.081, Florida Statutes, or other confidential materials contained on applicable pages of this application shall not be used or disclosed, except for evaluation purposes. However, if a contract is awarded to this offer or as a result in connection with the submission of this program, the Coalition shall have the right to use or disclose the information designated as trade secrets or confidential to the extent provided in the contract. This restriction does not limit the Coalition's right to use or disclose the information designated as trade secrets or designated as confidential which is obtained from another source."

Any exemption claimed will be limited to the pertinent documents and must be supported by a statutory exemption. Notwithstanding anything to the contrary, nothing contained in the application shall be deemed or interpreted to restrict or prevent the Coalition from complying with the disclosure requirements of Chapter 119, Florida Statutes, when material is incorrectly identified as a trade secret or confidential information. By submitting an application, the applicant covenants not to sue the Coalition and waives any

claim against the Coalition arising under Chapter 119, Florida Statutes or in connection with or as a result of any disclosures by the Coalition in connection herewith.

4.4 Monthly Invoicing and Payments

The Contractor shall submit invoices for payment **no later than the 13th of each month**. Unless the thirteenth (13th) falls on a Saturday, then, the invoice will be due the previous Friday, or if it falls on a Sunday, the invoice will be due the following Monday. Prior to final payment, invoices and back-up documentation must be received for all funds used. The Contractor agrees to submit requests for payment marked as an original to the Coalition's Procurement Department at monthly intervals, accompanied by such documentation as required by the Coalition and on the **13th** of the month, which is attached hereto and made a part hereof by this reference. Late submission by the Contractor may result in a delay in receipt of payment. Payments will not be authorized until the Coalition's Procurement Specialist has reviewed and approved a properly completed invoice with supporting documentation then received approval by the Chief Financial Officer. Invoices shall be submitted to via electronic copy to contractmanager@elcpolk.org referencing **ELCPOLK-FY2025-03**

4.5 Option to Request Price Adjustment

Prices shall remain firm for the first thirty-six (36) months of the resulting agreement. The awarded proposer will have an opportunity to request a price adjustment for any renewal periods this contract may be extended. The request for price adjustment must be submitted in writing no later than ninety (90) calendar days prior to the annual anniversary of the contract start date. The request for price adjustment must include written justification (i.e. labor increases, transportation increases, etc.) for the increase and a copy must be sent to contractmanager@elcpolk.org. The awarded vendor will only be allowed to submit one request for price adjustment per renewal year. Any approved request for price adjustment will not take effect until the annual anniversary of the contract start date and such price adjustment will be in effect for the 12-month period following said anniversary date. Written requests for price adjustments shall not exceed the rate of inflation determined by the Consumer Price Index (CPI) for U.S. All items, published by the U.S. Bureau of Labor Statistics appropriately adjusted for the calendar year (January 1st to December 31st) preceding the calendar year in which the request is made. Any price adjustment must be approved prior to the new price becoming effective.

4.6 Primary Point of Contact

The company shall identify a specific individual as a primary point of contact. This individual will be responsible for the company's work product. The individual shall be available within 24 hours' telephone notice to accomplish the following:

- Attend meetings
- Respond to telephone calls
- Respond to specific inquiries

4.7 Replacement of Personnel

The Coalition will be accepting the company's proposal based upon the Primary Point of Contact listed in the proposal. All changes to primary staffing are subject to the Coalition's approval. The replacement employee must have credentials similar to the employee replaced.

4.8 Work papers

The company shall retain all work papers for a period of at least 5 years. In addition, the company will provide the Coalition and or its assignees access, free of charge, copies of any or all work papers for a period of at least 5 years.

4.9 Insurance

1. **Contractor's Insurance:** The Contractor shall maintain liability insurance coverage on a comprehensive basis and always maintain such liability insurance during the term of this Contract and any renewal(s) and extension(s) of it. Unless it is a state agency or subdivision as defined by subsection 768.28(2), F.S., by execution of this Contract the Contractor accepts full responsibility for identifying and determining the type(s) and coverage policy limits of liability insurance necessary to provide reasonable financial protections for the Contractor and the clients to be served under this Contract. The limits of coverage under each policy maintained by the provider do not limit the provider's liability and obligations under this contract. Upon Contract execution, the Contractor shall furnish the Coalition's Procurement Specialist written verification supporting both the determination and existence of such insurance coverage. A self-insurance program established and operating under the laws of the State of Florida may provide such coverage. The Coalition reserves the right to require additional insurance.
2. **Workers' Compensation Insurance:** During the Contract term, the Contractor, at its sole expense, shall provide workers' compensation and employer's liability insurance of such a type and with such terms and limits as may be reasonably associated with the Contract, which, as a minimum, shall be: worker's compensation and employer's liability insurance in accordance with Chapter 440, F.S., with minimum employers' liability limits of \$100,000 per accident, \$100,000 per person, and \$500,000 policy aggregate. Such policy shall cover all of Contractor's employees engaged in any Contract work.
3. **Reemployment Compensation Insurance:** During the Term of this Contract, the Contractor must comply with the reporting and contribution payments required under Chapter 443, F.S., for all employees connected with the Statement of Work.
4. **Liability Insurance:** The Contractor will provide Premise Liability Insurance in an amount appropriate to the risk manifested by the Contractor's staff working in the space provided by the Coalition. This also includes the indemnification of the State for any liabilities set forth in Section 768.28, F.S. The Contractor shall require all subcontractors to list the Early Learning Coalition of Polk County as a named insured on their insurance policies and shall submit such documents prior to execution of this Contract.
5. The coalition shall require professional services firms to provide appropriate errors and omissions insurance to cover certain services upon its sole discretion.
6. **Insurance Policies:** All insurance policies required above shall be issued by a company authorized to do business under the laws of the State of Florida, with the following qualification:
 - a) The company must hold a valid Florida Certificate of Authority as shown in the latest "List of All Insurance Companies Authorized or Approved to Do Business in Florida" issued by the State of Florida Department of Insurance and are members of the Florida Guaranty Fund.

7. **Certificates of Insurance:** **Certificates** shall indicate no modification or change in insurance shall be made without thirty (30) days in advance notice to the certificate holder.

CERTIFICATE HOLDER MUST READ:

Early Learning Coalition of Polk County

115 S. Missouri Ave., Suite 501
Lakeland, FL 33815

Compliance with the foregoing requirements shall not relieve the Contractor of its obligation under this section or under any other section of this Contract.

8. The Contractor shall be responsible for assuring that the insurance certificate required in conjunction with this Section remains in force for the duration of the Term, including all Renewal Terms and/or additional phases or work that may be granted to the Contractor in accordance with this Agreement. If insurance certificates expire during the Term, the Contractor shall submit new or renewal insurance certificates to the Coalition at least thirty (30) calendar days before such expiration. In the event that expired certificates are not replaced with new or renewal certificates which cover the Term, the Coalition shall suspend the contract until such time as the new or renewed certificates are received by the Procurement Specialist; provided, however, that this suspended period does not exceed thirty (30) calendar days. If such suspension exceeds thirty (30) calendar days, the Coalition may terminate this Contract (as provided in Article II, Section H (4) (xi) hereof) and seek re-procurement damages from the Contractor, including legal fees.
9. The Contractor shall not commence any work in connection with this Contract until the Coalition's Procurement Specialist has approved Insurance. All insurance policies shall be with the insurers qualified to do business in Florida. The Coalition's Procurement Specialist shall be furnished proof of coverage of insurance by certificates of insurance accompanying the Contract documents and shall name the Coalition as an additional named insured. The Coalition shall be exempt from, and in no way liable for, any sums of money that may represent a deductible in any insurance policy or premium. The payment of such deductible shall be the sole responsibility of the Contractor providing such coverage.

4.10 Termination

1. **Termination at Will**

Either Party may terminate the resulting contract without cause upon thirty (30) days prior written notice to the other Party ("Notification Period") unless a sooner time is mutually agreed upon in writing. The Contractor shall be entitled to perform services and receive compensation for services performed during the Notification Period; provided, however, that the Coalition shall not be liable for payment for any services performed by the Contractor after the end of the Notification Period.

2. **Termination for Convenience**

The Coalition may terminate the resulting Contract at any time upon written notice to Contractor. The Contractor shall immediately cease performance of services upon written notice. The Coalition shall not be liable to the Contractor for any cancellation charges or lost profits. The Coalition shall only be liable to pay for services rendered up to the date of termination.

3. Termination for Lack of Funds

The Coalition may terminate the resulting Contract upon no less than twenty-four (24) hours' written notice to the Contractor for lack of availability or adequacy of funds. Termination of this Contract under this subsection shall not relieve the Coalition of its obligation to pay any amounts then due to Contractor up to the date of termination.

4. Termination for Cause

The Coalition may terminate the resulting Contract at any time, upon written notice, to the Contractor for "Cause". As used herein "Cause" means Contractor's:

- i. Failure to provide proof of licensure, certification or background screenings as required by the Coalition;
- ii. Failure to submit complete and accurate reports to the Coalition;
- iii. Refusal to allow the Coalition full access to records;
- iv. Refusal to allow the Coalition to monitor, evaluate and review programs;
- v. Failure to obey applicable laws pertaining to sexual harassment or discrimination;
- vi. Securing of obligations under this Contract by means of fraud, misrepresentation or material misstatement;
- vii. Failure to correct deficiencies discovered during a monitoring, evaluation or review by the Coalition or any governmental body within the period of time specified by the Coalition or governmental body;
- viii. Failure to give requisite notice pursuant to Article II, Section F (1) hereof;
- ix. Unsuccessful completion of the intervention and improvement program pursuant to Article III, Section G hereof;
- x. Failure to fulfill obligations pursuant to Article II, Section F hereof; or
- xi. Failure to provide insurance certificates pursuant to Article II, section F (7) hereof.

5. In the event of termination of the resulting Contract by either Party, the Coalition may require any or all of the following: (a) the return of all finished or unfinished documents, data studies, surveys, and reports prepared and secured by the Contractor under this Contract; (b) seek reimbursement of the Coalition funds paid to the Contractor under this Contract for unperformed services; or (c) terminate or cancel any other contracts entered into between the Parties.

4.11 Contractor Indemnification

1. Contractor agrees to indemnify, defend and hold harmless the Coalition and all of its affiliates and their officers, directors, shareholders, agents, employees, and successors from and against any liabilities, losses, damages, causes of action or injuries, together with costs and expenses, including attorneys' fees and costs, arising out of any act, actions, negligence or omissions, or breach of Article

It, hereof, by the Contractor and its directors, officers, agents, employees and Qualified Subcontractors during the performance or operation of this Contract. The Contractor's obligation to indemnify under this subsection will apply regardless of whether the claim arises in tort, contract, negligence, or otherwise.

2. The Coalition shall notify the Contractor in writing within seven (7) days of any claim for indemnification hereunder. The Coalition's failure to provide written notification to the Contractor shall not release the Contractor from its indemnification obligation.
3. Notwithstanding the foregoing, the indemnification provisions of this Section are not applicable to contracts executed by state agencies or subdivisions, as defined under Section 768.28, F.S., or any other Florida statute applicable to sovereign immunity.

4.12 Subcontracting

1. The Contractor agrees to neither assign the responsibility for the resulting Contract to another party nor subcontract for any of the work contemplated under the Contract without prior written approval of the Coalition, which shall not be unreasonably withheld. Any sublicense, assignment, or transfer otherwise occurring without prior approval of the Coalition, shall be null and void.
2. Unless otherwise stated in the resulting contract between the Contractor and qualified Subcontractor, the Contractor shall be responsible to make payments to any qualified Subcontractor within seven (7) working days after receipt of full or partial payments from the Coalition in accordance with Section 287.0585, F.S. Failure to pay within the foregoing statutory period or as provided by written contract, whichever is applicable, will result in a penalty that shall be charged against the Contractor and upon receipt shall be paid to the qualified Subcontractor in the amount of one-half of one percent (.005) of the amount due per day from the expiration of the period allowed for payment. Such a penalty shall be in addition to actual payments owed and shall not exceed fifteen (15%) percent of the outstanding balance due.

4.13 Gratuities

During the Term of this Contract and for a period of two (2) years subsequent to its expiration or termination for any reason, the Contractor will not offer to give or give any gift to any employee of the Coalition. The Coalition shall report the Contractor to the Department of Management Services for any violation of this Section for the potential inclusion of the Contractor's name on the suspended vendors list for an appropriate period. The Contractor shall ensure that any qualified Subcontractor's shall comply with this Section.

4.14 Force Majeure

Neither party shall be liable to the other for any delay or failure to perform under this Contract if such delay or failure is neither the fault nor the negligence of the party or its employees or agents and the delay is due directly to acts of God, wars, acts of public enemies, strikes, fires, floods, or other similar cause wholly beyond the party's control, or for any of the foregoing that affects subcontractors or suppliers if no alternate source of supply is available. However, in the event of delay from the foregoing causes, the Contractor shall take all reasonable measures to mitigate all resulting delay or disruption in the party's performance obligation under this Contract. If the delay is excusable under

this paragraph, the delay will not result in any additional charge or cost under the Contract to either party. In the case of any delay the Contractor believes is excusable under this paragraph, the Contractor shall notify the Coalition in writing of the delay or potential delay and describe the cause of the delay either: (1) within ten (10) calendar days after the cause that creates or will create the delay first arose, if the Contractor could reasonably foresee that a delay could occur as a result; or (2) within five (5) calendar days after the date the Contractor first had reason to believe that a delay could result, if the delay is not reasonably foreseeable. The foregoing shall constitute the Contractor's sole remedy or excuse with respect to delay. Providing notice in strict accordance with this paragraph is a condition precedent to such a remedy. The Coalition, in its sole discretion, will determine if the delay is excusable under this paragraph and will notify the Contractor of its decision in writing. No claim for damages, other than for an extension of time, shall be asserted against the Coalition. The Contractor shall not be entitled to an increase in the Contract price or payment of any kind from the Coalition for direct, indirect, consequential, impact, or other costs, expenses, or damages, including but not limited to costs of acceleration or inefficiency arising because of delay, disruption, interference, or hindrance from any cause whatsoever. If performance is suspended or delayed, in whole or in part, due to any of the causes described in this paragraph, after the causes have ceased to exist, the Contractor shall perform at no increased cost, unless the Coalition determines, in its sole discretion, that the delay will significantly impair the value of the Contract to the Coalition or the State, in which case, the Coalition may do any or all of the following: (1) accept allocated performance or deliveries from the Contractor, provided that the Contractor grants preferential treatment to the Coalition with respect to products or services subjected to allocation; (2) purchase from other sources (without recourse to and by the Contractor for the related costs and expenses) to replace all or part of the products or services that are the subject of the delay, which purchases may be deducted from the Contract quantity; or (3) terminate the Contract in whole or in part.

4.15 Effect of Prime Changes

The resulting Contract is issued pursuant to the provisions set forth in the Coalition's grant agreement with Florida's Division of Early Learning (DEL). If the DEL grant award is amended and the amendment causes this Contract to be inconsistent with or contrary to the grant award, the Parties hereto agree that they will, upon request, negotiate in good faith upon such amendments to this Contract as may be necessary to make this Contract consistent with the requirements of the DEL grant agreement.

V. PRICING FORM AND SPECIFICATIONS

Enter Specifications (if applicable) and Pricing below. Proposers must enter a Monthly Unit Price and a 3 Year Total Price in the space provided below for each item listed on the PRICING FORM AND SPECIFICATIONS, or the submitted proposal could be declared non-responsive. Additional (optional) services may be provided in item numbers 5-6. Pricing will remain fixed for the duration of the initial contract period.

Item Number	Location	Description	Additional Specifications (Write in)	Monthly Unit Price	3 Year Total Price
PRODUCT: Dedicated Fiber Internet Speed 200 Mbps (or equivalent)					
1	115 S. Missouri Avenue, Lakeland, FL Suite 201 & 501	Dedicated Internet Access (DIA)		\$ _____	\$ _____
2	115 S. Missouri Avenue, Lakeland, FL Suite 201 & 501	5 Static IPS		\$ _____	\$ _____
3	203 Avenue A NW, Winter Haven, FL Suite 101	Dedicated Internet Access (DIA)		\$ _____	\$ _____
4	203 Avenue A NW, Winter Haven, FL Suite 101	5 Static IPS		\$ _____	\$ _____
DISCOUNTS _____					
TOTAL \$ _____					

Additional Service -Write In (Optional)					
5	115 S. Missouri Avenue, Lakeland, FL Suite 201 & 501			\$_____	\$_____
6	203 Avenue A NW, Winter Haven, FL Suite 101			\$_____	\$_____
TOTAL					\$_____

ATTACHMENT A
Letter of Certification

The Early Learning Coalition of Polk County
Attn: Procurement
115 S. Missouri Ave., Suite 201
Lakeland, FL 33815

Dear Mrs. Clark:

We have read The Early Learning Coalition of Polk County's Request for Proposal and fully understand its intent. We certify full acceptance of the contents of this RFP. We certify that we have adequate personnel, equipment, technology, and facilities to fulfill the requirements of the engagement. We understand that our ability to meet the criteria and provide the required services will be judged by Coalition staff members and/or members of the Board.

I, the undersigned respondent, have not divulged, discussed, or compared this proposal with any other respondents and have not colluded with any other respondent in the preparation of this proposal in order to gain an unfair advantage in the award of this proposal.

If any officer, director or agent is also a Coalition employee, they are listed below. All companies must disclose the name of any Coalition employee who owns, directly or indirectly, any interest in the company's business or any of its branches. All companies must disclose any business relationships or family relations with any officer, board member, subcontractor, or employee of the Coalition.

Name: _____ Relationship: _____

It is understood that all information included in, attached to, or required by this RFP shall become public record upon their delivery to the Coalition as defined in the Public Records Act, Chapter 119, Florida Statutes.

Submitted by: _____

Name of Company: _____

Authorized Signature: _____ Date: _____

Title: _____

E-Mail: _____ Telephone: _____

ATTACHMENT B
CERTIFICATIONS AND ASSURANCES AFFIDAVIT

DIRECTIONS: BY ATTESTING TO THIS FORM, THE CONTRACTOR AGREES TO COMPLY WITH ALL SECTIONS ON THE SWORN AFFIDAVIT. THIS FORM MUST BE SIGNED IN THE PRESENCE OF A NOTARY PUBLIC OR OTHER OFFICER AUTHORIZED TO ADMINISTER OATHS.

APPLICATION ACCURACY

I do hereby certify that all facts, figures, and representations made in the proposal are true and correct. The filing of this proposal has been authorized by the contracting entity and I have been duly authorized to act as the representative of the organization in connection with this proposal. I also agree to follow all terms, conditions, and applicable federal law and state statutes.

AUTHORITY FOR DATA COLLECTION – 45 CFR Part 98.10-12; ss. 1001.213, 1002.75 and 1002.82, F.S.

In performing its responsibilities, the Contractor hereby certifies and assures that it will fully comply with the following requirements.

I. Federal certifications – applicable to all entities

II. Federal or state-required assurances – applicable to OEL subrecipients

- A. Assurances – Non-construction programs (OMB Standard Form SF 424 B)
- B. Assurances - construction programs (OMB Standard Form SF 424D), if applicable
- C. Assurances – TheTransparency Act (as defined by 2 CFR Part 170)
- D. Other miscellaneous/general disclosures
- E. Assurance for proper expenditure reporting
- F. CCDF Salary Cap annual testing requirements
- G. Certification (ACORN) - prohibition for distribution of funds to the Association of Community Organization for Reform Now
- H. Certification regarding ELC status as a non-major corporation
- I. Certification of cost allocation plan or indirect cost rate proposal
- J. Certification regarding separation of VPK Education Program and SR Program funds (ss. 1002.71(1) and (7), F.S., 1002.89, F.S., and 45 CFR part 98.54)
- K. Certification regarding subrecipient monitoring
- L. Certification regarding immigration status
- M. Certification regarding standards of conduct
- N. Clean Air Act (42 USC 7401, et seq.) and the Federal Water Pollution Control Act, as amended (33 USC 1251, et seq.)
- O. Conflicts of Interest
- P. Contract Work Hours and Safety Standards Act
- Q. Copeland “Anti-Kickback” Act (18 U.S.C. 874 and 40 U.S.C. 276c)
- R. Davis Bacon Act, as amended (40 USC 276a, et seq.)
- S. DUNS number – Data Universal Numbering System
- T. Equal Employment Opportunity (EEO)
- U. Procurement of recovered materials
- V. Procurements and other purchases
- W. Property
- X. Purchase of American-Made Equipment and Products
- Y. System for Award Management (SAM) Unique Entity Identifier Requirements
- Z. Trafficking Victims Protection Act of 2000

III. Federal certifications – applicable to all entities

The following Certifications are hereby adopted and incorporated herein by reference as if fully set forth herein. See 45 CFR 75 Appendix II, *Contract Provisions for Non-Federal Entity Contracts Under Federal Awards*.

FOR THOSE THAT REQUIRE SIGNATURE, SEE ATTACHED EXECUTED.

[Debarment Certification - Primary](#)

[Debarment Certification - Lower Tier](#)

[Environmental Tobacco Smoke Certification](#)

IV. Federal or state-required assurances – applicable to OEL subrecipients

The following Assurances are hereby adopted and incorporated herein by reference as if fully set forth herein.

A. **Assurances – non-construction programs** – required by OMB Standard Form SF 424 B, see [SF-424B Non-construction Programs](#).

B. **Assurances – construction programs** – required by OMB Standard Form SF 424D, see [SF-424D Construction Programs. – IF APPLICABLE](#)

Note – Certain of these assurances may not be applicable to the ELC's operations. Please contact OEL with questions.

C. **"The Transparency Act" (as defined in 2 CFR Part 170)**

The following award term is hereby adopted and incorporated herein by reference as if fully set forth herein –

HHS now requires this program award to adhere to the Transparency Act's Sub-award and Executive Compensation reporting requirements (as 2 CFR Part 170 defines). Under the Transparency Act, the grantee must report all sub-awards (as 2 CFR Part 170 defines) more than \$25,000, unless exempted. Please see the newly applicable Award Term for Federal Financial Accountability and Transparency Act at [the USDHHS ACF website](#).

D. **Other Assurances – miscellaneous/general disclosures**

As the ELC's duly authorized representative, I certify that the ELC –

1. Will use fiscal control and fund accounting procedures that will ensure proper disbursement of, and accounting for, federal and state funds paid to that agency under each program. Access to such records shall be made available to authorized representatives of U.S. governmental agencies, the Florida DOE, the Florida DFS and the Auditor General of the state of Florida for the purpose of program and fiscal auditing and monitoring.
2. Will cause the required financial and compliance audits to be performed in accordance with the Single Audit Act Amendments of 1996 and 2 CFR §200, Subpart F, *Audit Requirements*, and/or Section 215.97, Florida Statutes, Florida Single Audit Act, as applicable.
3. Will establish safeguards to prohibit employees and board members from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest or personal gain.

4. Will initiate and complete the work within the applicable time frame after receiving the awarding agency's approval.
5. Will administer each program covered by this agreement in accordance with all applicable laws, regulations, statutes, rules, policies, procedures and program requirements governing the program(s).
6. Will comply with all applicable requirements of all other federal and state laws, executive orders, regulations and policies governing each funded program.
7. Will submit such reports as described in Section D of this agreement to the Florida DOE, the U.S. DOE and the USDHHS to perform their duties. The ELC will maintain such fiscal and programmatic records and provide access to those records, as necessary, for those departments to perform their duties.
8. Will provide reasonable opportunities for systematic consultation with and participation of teachers, parents and other interested agencies, organizations and individuals, including education-related community groups and non-profit organizations, in the planning for and operation of each program.
9. Will make any application, evaluation, periodic program plan or report relating to each program readily available to parents and other members of the general public.
10. Will have/establish and maintain a proper accounting system in accordance with generally accepted accounting standards.
11. Will not expend funds under the applicable program to acquire equipment (including computer software) in any instance in which such acquisition results in a direct financial benefit to any organization representing the interests of the purchasing entity or its employees or any affiliate of such an organization.
12. Will comply with the requirements in 2 CFR Part 180, Government-wide Debarment and Suspension (Nonprocurement).
13. Will comply with all state and federal requirements, as applicable, for internal controls to ensure compliance with federal and state statutes, regulations, and terms and conditions of the award.
14. Will comply with Florida's Government-in-the-Sunshine Law (Chapter 286, Florida Statutes), that provides a right of access to meeting of boards, commissions and other governing bodies of state and local governmental agencies or authorities.
15. If applicable, after timely and meaningful consultation, the recipient will provide the opportunity for children enrolled in private, non-profit schools, and the educational personnel of such schools, equitable participation in the activities and services provided by these federal funds, and will notify the officials of the private schools of said opportunity. (Educational services or other benefits provided, including materials and equipment, shall be secular, neutral, and non-ideological. Expenditures for such services or other benefits shall be equal [consistent with the number of children to be served] to expenditures for programs of children enrolled in the public schools of the local educational agency.)

E. Assurance for proper expenditure reporting

In accordance with 2 CFR §200.415, *Required Certifications*, the official who is authorized to legally bind the Contractor must include the following certification on final fiscal reports or vouchers requesting payment.

"By signing the *General Assurances, Terms and Conditions for Participation in Federal and State Programs*, I certify to the best of my knowledge and belief that all applications submitted are true, complete, and accurate, for the purposes and objectives set forth in the contract. I am aware that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal or administrative penalties for false statements, false claims or otherwise."

F. CCDF Salary Cap annual testing requirements

The Consolidated Appropriations Act, 2012 (P.L. 112-74), enacted Dec. 23, 2011, limits the salary amount that ELCs may award and charge to grants and cooperative agreements that the Administration of Children and Families (ACF) funds.

ELCs may not use CCDF award funds to pay an individual's salary at a rate more than the annual maximum Executive Level II federal pay rate. The Federal Executive Pay Scale maximum annual Executive Level II salary for calendar year 2015 is \$183,300 and is accessible annually at [the U.S. Office of Personnel Management website](#). This amount reflects an individual's base salary without fringe benefits and income that an individual may earn outside of the duties to the applicant organization. The ELC shall apply this salary limitation to subawards/subcontracts under an ACF grant or cooperative agreement ([Child Care Development Grant Funds Program Specific Terms and Conditions for State and Territory Grantees, V.2013.1 \(12/2012\)](#)).

1. ELCs/ELC subrecipients may not use grant funds to pay for salary costs that exceed the CCDF cap.
2. ELCs/ELC subrecipients must allocate salaries that multiple funding sources pay and compare these calculations to received program benefits.
3. The ELC/ELC subrecipients should perform and document an annual analysis using W-2 data.
4. All CCDF-funded grantees and sub-grantees are responsible for assuring compliance with this provision. All such CCDF fund recipients and subrecipients are responsible for enforcing other impacted entities of this compliance requirement.
5. All CCDF-funded grantees shall comply with salary cap reporting requirements outlined in this section.

G. Certification (ACORN) – prohibition for distribution of funds to the Association of Community Organization for Reform Now

To comply with P.L. 111-117, the grantee may not distribute federal funds made available under this agreement to the Association of Community Organizations for Reform Now (ACORN) or its subsidiaries. In addition, the grantee may not provide federal funds to any covered organization as House of Representatives (H.R.) 3571, the Defund ACORN Act, defines.

H. Certification regarding non-profit organization status as a non-major corporation

In accordance with 2 CFR §200.415, *Required Certifications*, the non-profit organization as appropriate must certify it does not meet the definition of a major corporation. 2 CFR §200.414(a) defines major nonprofit organizations as those which receive more than \$10 million dollars in direct Federal funding.

_____ The Contractor is not a major nonprofit organization.

_____ The Contract is a major nonprofit organization.

I. Certification of cost allocation plan or indirect cost rate proposal

In accordance with 2 CFR §200.415, *Required Certifications*, the Contractor must certify the submitted cost allocation plan or indirect cost rate proposal, as instructed by the Office. OEL's current cost allocation plan guidance instructs that no indirect cost rates are required or used by the Office at this time since Florida's

early learning programs have administrative spending caps assigned by federal regulation and/or state statutes. For more details, please contact OEL.

J. Certification regarding separation of VPK Education Program and SR Program funds

Pursuant to ss.1002.71(1) and (7), F.S., s. 1002.89, F.S., and 45 CFR part 98.54, the VPK and SR Programs are independent programs that separate state and federal sources fund. All grantee expenditures made and fiscal records maintained shall reflect funds expenditure separation.

The grantee hereby certifies that –

It will expend all SR (Child Care Development Fund, TANF, Social Services Block Grant and General Revenue) funds solely for operating the SR Program and the funds shall be distinctive and clearly identifiable in all fiscal records the grantee maintains. The grantee shall use all state general revenue funds awarded for operating the Voluntary Prekindergarten Education Program solely operating the Voluntary Prekindergarten Education Program and shall be distinctive and clearly identifiable in all fiscal records the grantee maintains.

K. Certification regarding subrecipient monitoring

The grantee certifies that it has established and shall implement fiscal and programmatic monitoring procedures for its subrecipients.

L. Certification regarding immigration status

The grantee certifies that it agrees to comply with the provisions of s. 432 of the Personal Responsibility and Work Opportunity Reconciliation Act (42 USC part 1611); ensuring that only individuals eligible for CCDF services receive them.

M. Certification regarding standards of conduct

The grantee certifies that it shall comply with the provisions 2 CFR §200.318, General Procurement Standards, regarding standards of conduct. It will establish safeguards to prohibit employees and board members from using their positions for any purpose that constitutes or presents the appearance of personal or organizational conflict of interest or personal gain.

N. Clean Air Act and Federal Water Pollution Control Act

Pursuant to the Clean Air Act (42 U.S.C. 7401 et seq.) and the Federal Water Pollution Control Act (33 U.S.C. 1251 et seq.), as amended, if this grant or contract is in an amount in excess of \$100,000, **Contractor** shall comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401 et seq.) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251 et seq.). Violations shall be reported to the federal awarding agency and the Regional Office of the Environmental Protection Agency (**EPA**). See 45 CFR 75, Appendix II, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards.

O. Conflicts of Interest

1. Pursuant to 2 CFR §200.318, *General procurement standards*, the Office must maintain oversight to ensure contractors perform scoped services in accordance with minimum standards or conduct.

- 1.1. If the Contractor has a parent, affiliate or subsidiary organization that is not a state or local government the Contractor must also maintain written standards of conduct covering organization conflicts of interest.
 - 1.2. Organizational conflicts of interest mean that because of relationships with a parent company, affiliate, or subsidiary organization, the Contractor is unable or appears to be unable to be impartial in conducting a procurement action involving a related organization.
 - 1.3. The Contractor's written standards of conduct must also address the performance of employees engaged in the selection, award and administration of contracts.
2. Related party contracts. Pursuant to state statute and OEL instructions (s. 1002.84(20), F.S.), the Contractor shall provide OEL contract documentation for any contracts with Contractor employees, governing board members or relatives of either group as s. 112.3143(1)(b), F.S., defines. The Contractor must comply with disclosure and reporting requirements in state statute and OEL instructions (s. 1002.84(20), F.S.).
- 2.1. Any governing board member(s) benefitting from Contractor agreement(s) must disclose in advance the conflict of interest and must abstain from the vote process.
 - 2.2. The impacted individual must complete the necessary conflict of interest disclosure forms.
 - 2.3. The Contractor shall present all such contracts to the governing board for a vote. A valid approval requires two-thirds vote of the Contractor's board, a quorum must be established.
 - 2.4. The Contractor shall not enter into or execute a contract in excess of \$25,000 with a member of the governing board or relative of a board member without OEL's prior approval.
 - 2.5. The Contractor does not have to obtain OEL's prior approval for contracts below \$25,000.
 - 2.6. However, the Contractor must adequately disclose and properly report and track such contract activity.
 - 2.7. The Contractor shall report such contracts to OEL within 30 days after receiving approval from the governing board.

P. Contract Work Hours and Safety Standards Act

Federal and state standards for procurement and contracts administration require all contracts in excess of \$100,000 discuss requirements for compliance with federal labor laws. See 45 CFR 75 Appendix II, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards. This provision applies to agreements that include salaries for laborers and for all contracts for repairs, improvements or other construction activities.

—Contractors will compute wages on a 40-hour week and pay employees for extra hours worked. None shall be forced to work in unsanitary, hazardous or dangerous conditions or surroundings.

—These requirements do not apply to purchase of supplies or materials or articles ordinarily available on the open market or contracts for transportation services.

Q. Copeland "Anti-Kickback" Act (18 U.S.C. 874 and 40 U.S.C. 276c)

Federal and state standards for procurement and contracts administration require all contracts in excess of \$2,000 discuss requirements for compliance with federal labor laws. See 45 CFR 75 Appendix II, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards.

—This provision applies to agreements that include salaries for laborers and for all contracts for repairs, improvements or other construction activities.

—Each contractor or subrecipient shall be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he is otherwise entitled. The recipient shall report all suspected or reported violations to the Department of Labor.

R. Davis-Bacon Act, as amended (40 USC 276a, et.seq.)

When federal program legislation requires, all construction contracts of more than \$2,000 the recipients and subrecipients award shall include a provision for compliance with the Davis-Bacon Act (40 USC 276a, et seq.), as supplemented by Department of Labor (DOL) regulations (29 CFR Part 5, Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction). Under this Act, contractors shall be required to pay wages to laborers and mechanics at a rate not less than the minimum wages specified in a wage determination made by the Secretary of Labor. In addition, contractors shall be required to pay wages not less than once a week. The recipient shall place a copy of the DOL-issued current prevailing wage determination in each solicitation, and the award of a contract shall be conditioned upon the acceptance of the wage determination. The recipient shall report all suspected or reported violations to the federal awarding agency. DOL regulations, rules and instructions concerning implementation of the Davis-Bacon Act and other labor laws can be found at Title 29 CFR Part(s) 1, 3, 5, 6 and 7.

S. DUNS Number – Data Universal Numbering System

The federal government requires organizations to provide a DUNS number as part of their grant applications and proposals. The OMB has adopted the use of DUNS numbers to keep track of how federal grant money is awarded and dispersed. The DUNS number is a nine-digit number the Dun and Bradstreet Company issues. This company provides business information for credit, marketing and purchasing decisions. Some entities will also have what is known as “DUNS + 4,” which is used to identify specific units within a larger entity.

Registering for a DUNS number is free of charge with no obligation to purchase any products from the Dun and Bradstreet Company. An authorizing official of the organization should request the number. Generally, it only takes a day to obtain a DUNS number by phone (1-866-705-5711), while applications through [the Dun and Bradstreet website](#) can take up to 30 days.

All recipients and subrecipients funded with federal funds must obtain a DUNS number prior to receiving a grant

T. Equal Employment Opportunity (EEO)

The ELC agrees to comply with E.O. No. 11246, Equal Employment Opportunity (30 Federal Register (F.R.) 12319, 12935, 3 CFR, 1964-1965 comp. p. 339), Sept. 24, 1965, as E.O. 11375, Amending Executive Order 11246 Relating to Equal Employment Opportunity, of Oct. 13, 1967, amended, and as the Department of Labor regulations (41 CFR part 60) Office of Federal Compliance Programs, Equal Opportunity, Department of Labor supplements. See 45 CFR 75, Appendix II, *Contract Provisions for Non-Federal Entity Contracts Under Federal Awards*.

U. Procurement of Recovered Materials

(a) Pursuant to 2 CFR §§200.317, Procurements by states, and §200.322, Procurement of recovered materials, the ELC will comply with the following requirements of section 6002 of the Solid Waste Disposal Act.

- (i) procure only items designated in the guidelines of the Environmental Protection Agency (EPA) at 40 CFR Part 247 for buying recycled-content products;

- (ii) Procure solid waste management services in a manner that maximizes energy and resource recovery; and
- (iii) establish an affirmative procurement program for purchases of recovered materials identified in the EPA guidelines. Information about this requirement is available at EPA's Comprehensive Procurement Guidelines web site, <http://www.epa.gov/cpg/> . The list of EPA-designated items is available at <http://www.epa.gov/cpg/products.htm>.

(b) In accordance with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act, the ELC shall procure items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition. The ELC shall procure items designated in the EPA guidelines that contain the highest percentage of recovered materials practicable unless the ELC determines that such items: (1) are not reasonably available in a reasonable period of time; (2) fail to meet reasonable performance standards, which shall be determined on the basis of the guidelines of the National Institute of Standards and Technology, if applicable to the item; or (3) are only available at an unreasonable price.

(c) Paragraph (b) of this clause shall apply to items purchased under this contract where: (1) the ELC purchases in excess of \$10,000 of the item under this contract; or (2) during the preceding Federal fiscal year, the ELC: (i) purchased any amount of the items for use under a contract that was funded with federal appropriations and was with a Federal agency or a State agency or agency of a political subdivision of a State; and (ii) purchased a total of in excess of \$10,000 of the item both under and outside that contract.

V. Procurements and other purchases

The ELC must comply with federal/state procurement requirements. State procurement instructions are described in ss. 215.971, 287.057, and 287.058, F.S. However, the ELC is not required to competitively procure direct service providers for the SR or VPK Education Programs. The ELC must have documented procurement policies and procedures that meet the minimum requirements of federal rules and regulations which are located at 2 CFR §§200.317-200.326.

W. Property

1. Property purchased in whole or in part with federal funds shall be used for the purpose of that federal program and accounted for in accordance with applicable federal and state statutes, rules and regulations. The ELC shall comply with the provisions of 45 CFR §75.318 *Real property*, 45 CFR §75.320 *Equipment*, and 45 CFR §75.321 *Supplies*. The ELC shall include in all subrecipient contracts, and any vendor contracts for services that include purchasing/procuring equipment, language that requires property a subrecipient purchases with funds provided under the agreement to revert to the ELC upon contract termination. In accordance with OEL Program Guidance 240.02, title to all property acquired with funds provided to the ELC under this agreement shall be vested in the ELC; however, title and ownership shall be transferred to OEL upon termination of the ELC participation in early learning programs, unless otherwise authorized in writing by OEL. All property required to be returned to the Office will be in good working order. See 2 CFR §200.318, *General procurement standards*, s. 273.02, F.S., and 69I-73.002, F.A.C.
2. The term “nonexpendable property” shall include all tangible personal property which meet the criteria set forth in Rule 69I-73.002, F.A.C. In accordance with 45 CFR 75.439 and in compliance with [OEL Program Guidance 240.05, Guidance on Prior Approval Procedures for Selected Costs and Administrative Requirements](#), property shall not be purchased with program funds without prior approval from OEL (Exhibit 1 CC.).
3. Contingencies such as liens or other liabilities shall not be placed upon assets purchased with program funds, nor shall non-expendable property purchased with program funds be used as collateral.
4. In accordance with OEL Program Guidance 240.02 – Tangible Personal Property, the funding sources for the purchase of all such property shall be identified and all such property purchased in the performance of the Early Learning programs shall be listed on the property records of the ELC. The ELC shall inventory annually and maintain accounting records for all equipment purchased in accordance with OEL Program Guidance 240.02, relevant Florida Statutes, state rules, federal regulations and federal cost principles.
5. Based on Section 273.055, F.S., and Rules 69I-72.002, and 69I-73.005 F.A.C., when original or replacement equipment acquired by a subrecipient contractor is no longer needed for the original project or program or for other activities currently or previously supported by a federal agency, disposition of the equipment will be made as described below in 6.
6. The Office’s policy concerning proceeds received from the sale of property with a current per unit fair market value up to \$5,000 is the net amount received from such sales will remain at the ELC level to be used in the same ongoing program. Funds from such sales will be treated as other program income in the same ongoing program(s). This type of income must be amended into a current year's program budget in which the sale occurred. It should then be reported in accordance with OEL Program Guidance 240.01. This identification of income is necessary to meet reporting requirements of the United States Department of Health and Human Services. Complete documentation for this type of income and expenditures must be maintained for monitoring and auditing purposes. If the ELC is no longer receiving funds for the particular project or program, the income from such equipment sales will be returned to the Office to be forwarded to the United States Department Health and Human Services.¹ Equipment that was initially purchased with federal funds with a

current per-unit fair market value in excess of \$5,000, must be processed in accordance with 2 CFR §200.313(e)(2), *Equipment*, with the assistance and prior written approval of the Office.

¹ *Upon termination of a project, and at the discretion of the Office, all equipment/property purchased with project funds will be transferred to the location(s) specified by the Office and all necessary actions to transfer the ownership records of the equipment/property to the Office or its designee, will be taken.*

X. Purchase of American-made Equipment and Products

The ELC agrees that, to the greatest extent practicable, all equipment and products purchased with funds made available by this agreement will be American-made.

P. L. 103-333, the Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Act of 1995, § 507 – “It is the sense of the Congress that, to the greatest extent practicable, all equipment and products purchased with funds made available in this Act should be American-made.”

Y. System for Award Management (SAM)

Unless exempt from these requirements under OMB guidance at 2 CFR Part 25 (e.g., individuals), the Contractor must:

1. Be registered in SAM prior to submitting an application or proposal under this announcement. SAM information can be found at <https://www.sam.gov/portal/public/SAM/>.
2. Maintain an active SAM registration with current information at all times during which it has an active Federal award or an application or proposal under consideration by a Federal awarding agency, and
3. Provide a valid unique entity identifier in its application (e.g., provide its DUNS number in each application or proposal it submits to the agency). Unique entity identifier means the identifier required for SAM registration to uniquely identify business entities.

Z. Trafficking Victims Protection Act of 2000 – (TVPA)

[Human Trafficking Requirements](#) are hereby adopted and incorporated herein by reference as if fully set forth herein. (22 U.S.C. 7104(g), as amended)

AGENCY CERTIFICATION

I, the undersigned applicant, hereby attest that the following policies, procedures, regulations, and documentation are in effect and agree to provide copies of the following within three working days of notification by the Coalition of intent to award the contract:

- Affirmative Action Policy
- Certified Minority Business Enterprises (if applicable)
- Small Disadvantaged Business Enterprise Policy (if applicable)
- Americans with Disabilities Policy
- Drug Free Workplace Policy

PUBLIC ENTITY CRIME AFFIDAVIT

I understand that a “public entity crime” as defined in Paragraph 287.133(l)(g), Florida Statutes means a violation of any state or federal law by a person with respect to and directly related to the transaction of business with any entity, agency or political subdivision of any other state or with the United States, including, but not limited to, any bid or contract for goods or services to be provided to any public entity or an agency or political subdivision of any other state or of the United States and involving antitrust, fraud, theft, bribery, collusion, racketeering, conspiracy, or material misrepresentation.

I understand that “convicted” or “conviction” as defined in Paragraph 287.133(l)(b), Florida Statutes means a finding of guilt or a conviction of a public entity crime with or without adjudication of guilt, in any federal or state trial court of record relating to charges brought by indictment after July 1989, or as a result of a jury verdict, non-jury trial, or entry of a plea of guilty or nolo contendere.

I understand that an “affiliate” as defined in Section 287.122, Florida Statutes means:

A predecessor or successor of a person convicted of a public entity crime; or an entity under the control of any natural person who is active in the management of the entity and who has been convicted of a public entity crime. The term “affiliate” includes those officers, directors, executives, partners, shareholders, employees, members, and agents who are active in the management of the affiliate.

The ownership by one person of shares constituting a controlling interest in another person, or pooling of equipment or income among persons when not for fair market value under an arm’s length agreement, shall be a prima facie case that one person controls another person. A person who knowingly enters into a joint venture with a person who has been convicted of a public entity crime in Florida during the preceding 36 months shall be considered an affiliate.

I understand that a “person” as defined in Section 287.133 Florida Statutes means any natural person or entity organized under the laws of any state or of the United States with the legal power to enter into a binding contract and which bids or applies to bid on contracts for the provision of goods or services let by a public entity, or which otherwise transacts or applies to transact business with a public entity. The term “person” includes those officers, directors, executives, partners, shareholders, employees, members, and agents who are active in management of an entity.

Based on information and belief, the statement which I have marked below is true in relation to the entity submitting this sworn statement. (Please indicate which statement applies.)

____ Neither the entity submitting this sworn statement, nor any officer, directors, executives, partners, shareholders, employees, members, or agents who are active in the management of the entity, nor any affiliate of the entity have been charged and convicted of a public entity crime subsequent to July 1, 1989.

____ The entity submitting this sworn statement, or one or more of the officers, directors, executives, partners, shareholders, employees, members or agents who are active in management of the entity, or an affiliate of the entity has been charged with and convicted of a public entity crime subsequent to July 1, 1989, and (Please indicate which additional statement applies)

____ There were proceedings concerning the conviction before a hearing officer of the State of Florida, Division of Administrative Hearings. The final order entered by the hearing officer did not place the person or affiliate on the convicted vendor list.

____ The person or affiliate was placed on the convicted vendor list. There has been a subsequent proceeding before a hearing officer of the State of Florida, Division of Administrative Hearings. The final

order entered by the hearing officer determined that it was in the public interest to remove the person or affiliate from the convicted vendor list. (Please attach a copy of the final order).

_____The person or affiliate has not been placed on the convicted vendor list. (Please describe any action taken by or pending in the Department of General Services).

ORGANIZATION'S NAME AND ADDRESS:

NOTE: AS EVIDENCED BY MY SIGNATURE BELOW, I UNDERSTAND AND WILL COMPLY WITH ALL TERMS AND CONDITIONS STATED HEREIN:

Type Authorized Official's Name

Authorized Official's Title

Authorized Official's Signature

Date

Federal Employee Identification Number

ATTACHMENT C

**CERTIFICATION REGARDING DEBARMENT, SUSPENSION AND OTHER RESPONSIBILITY MATTERS
(PRIMARY)**

Certification Regarding Debarment, Suspension, and Other Responsibility Matters--Primary Covered Transactions

Instructions for Certification

1. By signing and submitting this proposal, the prospective primary participant is providing the certification set out below.
2. The inability of a person to provide the certification required below will not necessarily result in denial of participation in this covered transaction. The prospective participant shall submit an explanation of why it cannot provide the certification set out below. The certification or explanation will be considered in connection with the department or agency's determination whether to enter into this transaction. However, failure of the prospective primary participant to furnish a certification or an explanation shall disqualify such person from participation in this transaction.
3. The certification in this clause is a material representation of fact upon which reliance was placed when the department or agency determined to enter into this transaction. If it is later determined that the prospective primary participant knowingly rendered an erroneous certification, in addition to other remedies available to the Federal Government, the department or agency may terminate this transaction for cause or default.
4. The prospective primary participant shall provide immediate written notice to the department or agency to which this proposal is submitted if at any time the prospective primary participant learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.
5. The terms covered transaction, debarred, suspended, ineligible, lower tier covered transaction, participant, person, primary covered transaction, principal, proposal, and voluntarily excluded, as used in this clause, have the meanings set out in the Definitions and Coverage sections of the rules implementing Executive Order 12549. You may contact the department or agency to which this proposal is being submitted for assistance in obtaining a copy of those regulations.
6. The prospective primary participant agrees by submitting this proposal that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is proposed for debarment under 48 CFR part 9, subpart 9.4, debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency entering into this transaction.
7. The prospective primary participant further agrees by submitting this proposal that it will include the clause titled "Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion-Lower Tier Covered Transaction," provided by the department or agency entering into this covered transaction, without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.
8. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not proposed for debarment under 48 CFR part 9, subpart 9.4, debarred, suspended, ineligible, or voluntarily excluded from the covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the

eligibility of its principals. Each participant may, but is not required to, check the List of Parties Excluded from Federal Procurement and Nonprocurement Programs.

9. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.
10. Except for transactions authorized under paragraph 6 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is proposed for debarment under 48 CFR part 9, subpart 9.4, suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal Government, the department or agency may terminate this transaction for cause or default.

Certification Regarding Debarment, Suspension, and Other Responsibility Matters--Primary Covered Transactions

1. The prospective primary participant certifies to the best of its knowledge and belief, that it and its principals:
 - (a) Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any Federal department or agency;
 - (b) Have not within a three-year period preceding this proposal been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;
 - (c) Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State or local) with commission of any of the offenses enumerated in paragraph (1)(b) of this certification; and
 - (d) Have not within a three-year period preceding this application/proposal had one or more public transactions (Federal, State or local) terminated for cause or default.
2. Where the prospective primary participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal.

Signature of Authorized Certifying Official

Printed Name and Title

Organization

ATTACHMENT D

CERTIFICATION REGARDING DEBARMENT, SUSPENSION AND OTHER RESPONSIBILITY MATTERS (LOWER TIER)

Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion--Lower Tier Covered Transactions

Instructions for Certification

1. By signing and submitting this proposal, the prospective lower tier participant is providing the certification set out below.
2. The certification in this clause is a material representation of fact upon which reliance was placed when this transaction was entered into. If it is later determined that the prospective lower tier participant knowingly rendered an erroneous certification, in addition to other remedies available to the Federal Government the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.
3. The prospective lower tier participant shall provide immediate written notice to the person to which this proposal is submitted if at any time the prospective lower tier participant learns that its certification was erroneous when submitted or had become erroneous by reason of changed circumstances.
4. The terms covered transaction, debarred, suspended, ineligible, lower tier covered transaction, participant, person, primary covered transaction, principal, proposal, and voluntarily excluded, as used in this clause, have the meaning set out in the Definitions and Coverage sections of rules implementing Executive Order 12549. You may contact the person to which this proposal is submitted for assistance in obtaining a copy of those regulations.
5. The prospective lower tier participant agrees by submitting this proposal that, [[Page 33043]] should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is proposed for debarment under 48 CFR part 9, subpart 9.4, debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency with which this transaction originated.
6. The prospective lower tier participant further agrees by submitting this proposal that it will include this clause titled ``Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion-Lower Tier Covered Transaction," without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.
7. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not proposed for debarment under 48 CFR part 9, subpart 9.4, debarred, suspended, ineligible, or voluntarily excluded from covered transactions, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the List of Parties Excluded from Federal Procurement and Nonprocurement Programs.
8. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and

information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

9. Except for transactions authorized under paragraph 5 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is proposed for debarment under 48 CFR part 9, subpart 9.4, suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal Government, the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.

Certification Regarding Debarment, Suspension, Ineligibility an Voluntary Exclusion--Lower Tier Covered Transactions

1. The prospective lower tier participant certifies, by submission of this proposal, that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency.
2. Where the prospective lower tier participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal.

Signature of Authorized Certifying Official

Printed Name and Title

Organization

ATTACHMENT E

CERTIFICATION REGARDING ENVIRONMENTAL TOBACCO SMOKE

The Pro-Children Act of 2001, 42 U.S.C. 7181 through 7184, imposes restrictions on smoking in facilities where Federally-funded children's services are provided. HHS grants are subject to these requirements only if they meet the Act's specified coverage. The Act specifies that smoking is prohibited in any indoor facility (owned, leased, or contracted for) used for the routine or regular provision of kindergarten, elementary, or secondary education or library services to children under the age of 18. In addition, smoking is prohibited in any indoor facility or portion of a facility (owned, leased, or contracted for) used for the routine or regular provision of federally funded health care, day care, or early childhood development, including Head Start services to children under the age of 18. The statutory prohibition also applies if such facilities are constructed, operated, or maintained with Federal funds. The statute does not apply to children's services provided in private residences, facilities funded solely by Medicare or Medicaid funds, portions of facilities used for inpatient drug or alcohol treatment, or facilities where WIC coupons are redeemed. Failure to comply with the provisions of the law may result in the imposition of a civil monetary penalty of up to \$1,000 per violation and/or the imposition of an administrative compliance order on the responsible entity.

Signature of Authorized Certifying Official

Printed Name and Title

Organization

ATTACHMENT F

CERTIFICATION REGARDING DRUG-FREE WORKPLACE REQUIREMENTS

INSTRUCTIONS

1. By signing and/or submitting this application or grant agreement, the grantee is providing the certification set out below.
2. The certification set out below is a material representation of fact upon which reliance is placed when the Contract is entered into. If it is later determined that the Contractor knowingly rendered a false certification, or otherwise violates the requirements of the Drug-Free Workplace Act, the agency, in addition to any other remedies available to the Federal Government, may take action authorized under the Drug-Free Workplace Act.
3. Workplace identifications must include the actual address of buildings (or parts of buildings) or other sites where work under the Contract takes place. Categorical descriptions may be used (e.g., all vehicles of a mass transit authority or State highway department while in operation, State employees in each local unemployment office, performers in concert halls or radio studios).
4. If the workplace identified to the Division of Early Learning changes during the performance of the Contract, the Contractor shall inform the Contract Manager of the change(s), if it previously identified the workplaces in question.
5. Definitions of terms in the Nonprocurement Suspension and Debarment common rule and Drug-Free Workplace common rule apply to this certification. Contractors' attention is called, in particular, to the following definitions from these rules:

Controlled substance means a controlled substance in Schedules I through V of the Controlled Substances Act (21 U.S.C. 812) and as further defined by regulation (21 CFR 1308.11 through 1308.15);

Conviction means a finding of guilt (including a plea of nolo contendere) or imposition of sentence, or both, by any judicial body charged with the responsibility to determine violations of the federal or state criminal drug statutes;

Criminal drug statute means a federal or non-federal criminal statute involving the manufacture, distribution, dispensing, use, or possession of any controlled substance;

Employee means the employee of a grantee directly engaged in the performance of work under a grant, including: (i) All direct charge employees; (ii) All indirect charge employees unless their impact or involvement is insignificant to the performance of the grant; and, (iii) Temporary personnel and consultants who are directly engaged in the performance of work under the grant and who are on the grantee's payroll. This definition does not include workers not on the payroll of the grantee (e.g., volunteers, even if used to meet a matching requirement; consultants or independent contractors not on the grantee's payroll; or employees of subrecipients or subcontractors in covered workplaces).

The Contractor certifies that it will or will continue to provide a drug-free workplace by:

(a) Publishing a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance is prohibited in the grantee's workplace and specifying the actions that will be taken against employees for violation of such prohibition;

(b) Establishing an ongoing drug-free awareness program to inform employees about --

1. The dangers of drug abuse in the workplace;
2. The grantee's policy of maintaining a drug-free workplace;
3. Any available drug counseling, rehabilitation, and employee assistance programs; and
4. The penalties that may be imposed upon employees for drug abuse violations occurring in the workplace;

(c) Making it a requirement that each employee to be engaged in the performance of the grant be given a copy of the statement required by paragraph (a);

(d) Notifying the employee in the statement required by paragraph (a) that, as a condition of employment under the grant, the employee will --

1. Abide by the terms of the statement; and
2. Notify the employer in writing of his or her conviction for a violation of a criminal drug statute occurring in the workplace no later than five calendar days after such conviction;

(e) Notifying the Division of Early Learning in writing, within ten (10) calendar days after receiving notice under paragraph (d)(2) from an employee or otherwise receiving actual notice of such conviction. Employers of convicted employees must provide notice, including position title, to every grant officer or other designee on whose grant activity the convicted employee was working, unless the federal agency has designated a central point for the receipt of such notices. Notice shall include the identification number(s) of each affected Contract;

(f) Taking one of the following actions, within 30 calendar days of receiving notice under paragraph (d)(2), with respect to any employee who is so convicted --

1. Taking appropriate personnel action against such an employee, up to and including termination, consistent with the requirements of the Rehabilitation Act of 1973, as amended; or
2. Requiring such employee to participate satisfactorily in a drug abuse assistance or rehabilitation program approved for such purposes by a federal, state, or local health, law enforcement, or other appropriate agency;

(g) Making a good faith effort to continue to maintain a drug-free workplace through implementation of paragraphs (a), (b), (c), (d), (e) and (f).

Dedicated Internet

The Contractor may insert in the space provided below the site(s) for the performance of work done in connection with the specific Contract:

Place of Performance (Street address, city, county, state, zip code)

Check if there are workplaces on file that are not identified here. ☐

Signature of Authorized Certifying Official: _____

Printed Name: _____
Title: _____
Date: _____

ATTACHMENT G

CERTIFICATION OF FILING AND PAYMENT OF FEDERAL TAXES

As required by the Departments of Labor, Health and Human Services, and Education and Related Agencies Appropriation Act, 2008 (Public Law 110-161, Division G, Title V, section 523), as a prospective financial assistance recipient entering into a grant or cooperative agreement of more than \$5,000,000, I, as the duly authorized representative of the applicant, do hereby certify to the best of my knowledge and belief, that:

1. The applicant has filed all federal tax returns required during the three years preceding this certification;

AND

2. The applicant has not been convicted of a criminal offense pursuant to the Internal Revenue Code of 1986 (U.S. Code – Title 26, Internal Revenue Code);

AND

3. The applicant has not, more than 90 days prior to this certification, been notified of any unpaid federal tax assessment for which the liability remains unsatisfied, unless the assessment is the subject of an installment agreement or offer in compromise that has been approved by the Internal Revenue Service and is not in default, or the assessment is the subject of a non-frivolous administrative or judicial proceeding.

Signature of Authorized Certifying Official: _____

Printed Name:

Title:

Date:

ATTACHMENT H

ACCEPTABLE USE POLICY

1.0 Policy Statement:

Members of the Florida Department of Education (FFDOE) workforce are responsible for compliance with state, federal, and local laws and the department's policies regarding information technology (IT) use and resource security. Technologies provided by the Department to members of the FFDOE workforce are for official business use to enable users to carry out the goals, objectives, and mandates of the department.

This policy serves as a notice that the department reserves the right to track user Internet, email, computer accesses, and telephone usage. FFDOE monitors network, server, and workstation activity, therefore, members of the FFDOE workforce must understand that use of FFDOE IT resources is subject to active monitoring.

In accordance with Section 282.318, Florida Statutes, all department workers are required to read and sign the form found at the end of this policy.

Any violations of the policies herein are grounds for disciplinary action including dismissal.

2.0 Policy Scope:

This policy applies to all workforce members granted access to FFDOE information systems and information assets, including full and part-time employees, temporary workers, volunteers and contactors. Those employed by others to perform FFDOE work are covered by this policy and shall comply with this and associated policies, procedures and guidelines. Devices covered under this policy include personal devices if the workforce member accesses or utilizes information assets and/or the department's network or technology resources with those devices.

3.0 Definitions:

- 3.1 Agency network - A collection of devices and networks interconnected so that the aggregate collection operates as a single network entity which is isolated via one or more perimeter devices (i.e., firewalls, routers) from other networks which do not belong to or are not a part of the agency network. Isolated demilitarized zones (DMZs) or interagency red zones normally are not considered part of the agency network; however, DMZs for which connectivity to non-agency networks is run through the agency network, or that have connectivity to the agency network are considered part of the agency network. Connectivity to the agency network is not intended for guest wireless services.
- 3.2 Anti-malware software - Software installed on a computing device that protects it from malicious software.
- 3.3 Anti-spyware - Program designed to remove or block spyware (computer software that collects personal information about users without their informed consent).
- 3.4 Anti-virus software - Computer programs that attempt to identify, thwart, and eliminate computer viruses and other malicious software (malware).
- 3.5 Authentication - The process of verifying that a user, process, or device is who or what it purports to be. Techniques fall into one of three categories: (1) something the user knows, such as a password or PIN; (2) something the user has, such as a smartcard or ATM card; and (3) something that is part of the user, such as a fingerprint, voice pattern, or retinal scan.
- 3.6 Authorization - Official or legal permission or approval.
- 3.7 Availability - The principle that authorized users have access to information and assets when required.
- 3.8 BIOS (Basic Integrated Operating System) - Refers to the software code run by a computer when first powered on. The primary function of the BIOS is to prepare the machine so other software programs stored on various media (such as hard drives, floppies, and CDs) can load, execute, and assume control of the computer.

Dedicated Internet

- 3.9 Blogging - A Web site that contains an online personal journal with reflections, comments and often hyperlinks provided by the writer.
- 3.10 Breach – Unlawful and/or unauthorized access of computerized data that materially compromises the security, confidentiality, or integrity of personal information.
- 3.11 Cable lock - A physical security device connecting the mobile device to an immovable object to deter theft.
- 3.12 Chief Information Officer - The person who coordinates all information resource management activities and information technology assets to ensure they are appropriately planned and managed in accordance with the agency mission.
- 3.13 Cloud Computing - Cloud computing in its simplest form refers to information technology services, accessed via the Internet, where the location of the infrastructure is unknown to the user. Some examples of cloud services are Microsoft Hotmail, Gmail, Facebook, Dropbox, and YouTube, although there are many more. Most of these popular cloud services are free.
- 3.14 Confidentiality - The principle that information is accessible only to those authorized to have access.
- 3.15 Configuration - Documentation of the specific rules or settings used in setting up agency hardware, software, and operating systems.
- 3.16 Email header – In an email, the header lines indicating sender, recipient, subject, sending time stamp, receiving time stamp of all intermediate and the final mail transfer agents and much more precede the text (body).
- 3.17 Encryption - The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy.
- 3.18 Enterprise Configuration Manager (ECM) Agent – an agent that runs on FDOE workstations to collect system data, not user data.
- 3.19 Extranet - An intranet that is partially accessible to authorized persons outside of a company or organization.
- 3.20 Family Educational Rights and Privacy Act (FERPA) - Federal standards protecting the privacy of education records.
- 3.21 FDOE internal network - See definition for agency network.
- 3.22 FDOE Personnel Management - The FDOE Bureau of Personnel Management, formally known as the Personnel Office.
- 3.23 Guest Wireless – A separate network intended for wireless internet connectivity by FDOE users and guests. Users of this network are not able to connect to the FDOE internal network.
- 3.24 Hardware - The mechanical, magnetic, electronic, and electrical devices comprising a computer system, such as the CPU, disk drives, keyboard, or screen.
- 3.25 Host-based IDS (Intrusion Detection System) - A special category of an Intrusion- Detection System (detects unwanted manipulations to computer systems, mainly through the Internet) that focuses its monitoring and analysis on the internal interfaces of a computing system rather than on its external interfaces.
- 3.26 Inappropriate material - Defined as text, photographic images, graphic representations or video materials that include but are not necessarily limited to: profane, scandalous, pornographic, suggestive or explicit sexual content; harassing messages; abusive, offensive, vulgar, obscene, or otherwise unprofessional content; or content related to chain letters, gambling, wagering, betting or other activity related to a game of chance, trial, contest, or sporting event.
- 3.27 Information Security Manager (ISM) - The person designated to administer the agency's information resource security program and plans in accordance with Section 282.318, Florida Statutes, and the agency's internal and external point of contact for information security matters.
- 3.28 Information Technology Resources - Agency computer hardware, software, networks, devices, connections, applications, and data. This can also include video equipment, audio equipment, telephones, fax machines, copiers, cell phones, pagers, and other technology-oriented devices.
- 3.29 Information Technology Worker – an agency user whose job duties and responsibilities specify development, maintenance, or support of information technology resources (see definitions for User, Worker, and Workforce).

Dedicated Internet

- 3.30 Integrity - The principle that assures information remains intact, correct, and authentic. Protecting the integrity involves preventing unauthorized creation, modification, or destruction of information.
- 3.31 Internal network - See definition for agency network.
- 3.32 Internet - A vast computer network linking smaller computer networks worldwide.
- 3.33 Intranet - A computer network with restricted access, as within a company, that uses software and protocols developed for the Internet.
- 3.34 Local Area Network (LAN) - A system for linking a number of microcomputers, terminals, workstations, etc., with each other or with a mainframe computer in order to share data, printers, information, programs, disks, etc.; usually confined to one office, building, or agency.
- 3.35 Malware - Software, such as viruses, worms, or Trojan horses intended to damage or disable a computer system. It can also include spyware that covertly obtains information from a computer. The term is short for malicious software.
- 3.36 Media - A storage vessel for electronic data and information (e.g., hard drive, laptop, CD, tape, thumb drive).
- 3.37 Mobile Computing Device - A laptop, smart phone, or other portable device that can process data.
- 3.38 Mobile Devices - A general term describing both mobile computing and mobile storage devices.
- 3.39 Mobile Storage Device - Portable data storage media including, but not limited to, external hard drives, thumb drives, floppy disks, recordable compact discs (CD- R/RW), recordable digital videodiscs (DVD-R/RW), iPods, media players, cell phones, or tape drives that may be easily attached to and detached from computing devices.
- 3.40 Modem - An electronic device that makes possible the transmission of data to or from a computer via telephone or other communication lines.
- 3.41 Need-to-Know – The principle that individuals are authorized to access only specific information needed to accomplish their individual job duties.
- 3.42 Network - A system containing any combination of computers, computer terminals, printers, audio or visual display devices, or telephones interconnected by telecommunication equipment or cables used to transmit or receive information.
- 3.43 Network Interface Card (NIC) - An adapter circuit board installed in a computer to provide a physical connection to a network.
- 3.44 Online storage – see Cloud Computing.
- 3.45 Password - A form of secret authentication data that is used to control access to a resource.
- 3.46 Personal firewall - Software installed on a computer or device which helps protect that system against unauthorized access.
- 3.47 Port scanning - When a software tool is used to search a network host for open ports. This is often used by administrators to check the security of their networks and by malicious users to compromise it.
- 3.48 Public information - All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency which is not confidential and has not been exempted from public disclosure by statute.
- 3.49 Public records - All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency. Section 119.011(12), F.S.
- 3.50 Real-time scanning - A feature of many anti-malware programs which monitor computer systems for suspicious activity such as viruses, spyware, adware, and other malicious objects in 'real-time' i.e., while surfing the web or running an application.
- 3.51 Short Message Service (SMS) - SMS stands for short message service. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone.

Dedicated Internet

- 3.52 Signature file - Pattern file used by anti-malware programs to identify existing malware. Out-of-date signature files will allow newer malware threats to go unnoticed.
- 3.53 SMS - See definition for Short Message Service.
- 3.54 Sniffing - Capturing network data.
- 3.55 Social media - Forms of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos).
- 3.56 Standards - A specific set of practices or procedures to regulate how a system or organization provides services.
- 3.57 Text messaging - Sending short text messages to a device such as a cellular phone, PDA or pager. Text messaging is used for messages that are no longer than a few hundred characters. The term is usually applied to messaging that takes place between two or more mobile devices.
- 3.58 Transitory - Transitory messages are those intended to communicate information of short-term value. Examples of transitory messages include: reminders about scheduled meetings or appointments; most telephone messages; notifications such as "I will be 10 minutes late," etc. "Transitory" refers to short-term value based upon the content and purpose of the message, not the format or technology used to transmit it. Transitory messages are not intended to formalize or perpetuate knowledge.
- 3.59 Trojan horse - A malicious program that is disguised as or embedded within legitimate software.
- 3.60 User - Any authorized entity that uses information technology resources (see definitions for Worker, Workforce, and Information Technology Worker).
- 3.61 Virus - A parasitic software program, equipped with the means of reproducing itself, which spreads throughout a computer or network by attaching itself or infecting other software or diskettes. A worm is a similar program that propagates across a network by making copies of itself.
- 3.62 VPN Access – Access to the FFDOE network through a network, device or medium that is not controlled by FFDOE.
- 3.63 Virtual Private Network (VPN) - A network service that ensures data is private and secure (using encryption) when connected to an untrusted public network such as when using home internet service or public Wi-Fi hotspots.
- 3.64 VPN Client – Software loaded on a user's laptop, tablet or desktop computer that provides a secure connection to the FFDOE network.
- 3.65 Wireless Access Point (WAP or AP) - A device that connects wireless communication devices together to form a wireless network. The WAP usually connects to a wired network and can relay data between wireless devices and wired devices.
- 3.66 Wireless network - A computing network made up of, but not limited to, computers and access points or repeaters joined by radio communication using a frequency spread-spectrum technology.
- 3.67 Worker – A member of the workforce, a worker may or may not use information technology resources (see definitions for User, Workforce, and Information Technology Worker).
- 3.68 Workforce - Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct or contractual control of the department, whether or not they are paid by the agency (see definitions for User, Worker, and Information Technology Worker).
- 3.69 Workstation - A computer used by members of the workforce for work-related duties.
- 3.70 Worm - A self-replicating computer program. It uses a network to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user intervention. Unlike a virus, it FDOEs not need to attach itself to an existing program. Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.

4.0 Guidelines:

You should direct questions regarding this policy to the Department of Education Information Security Manager (ISM).

FFDOE Policies referenced in this document should be reviewed and understood if applicable to the user. Additional reference policies are as follows:

- Computer Security Incident Response.
- Data Classification.

5.0 Procedures:

5.1 Compliance with Applicable Laws

5.1.1 It is the responsibility of the user having access to the information technology (IT) resources and databases of the Florida Department of Education (FDOE) and the State of Florida (State) to read and understand the department's policies and procedures regarding the acquisition of resources, disposal of resources, the security of data and resources (see the Department's Code of Personal Responsibility). All members of the FDOE Workforce are to abide by all of the policies and procedures. The willful and knowing of unauthorized use, alteration or destruction of IT resources and databases is a computer-related crime punishable under Chapter 815, F.S.

5.1.2 Each member of the FDOE workforce is responsible for complying with applicable state and Federal security rules and laws and with the agency's security policies and procedures when performing agency work or when using agency information technology resources.

5.2 Computer Use and Confidentiality Agreement

5.2.1 Each member of the FDOE workforce is to acknowledge, in writing, these responsibilities by completing an agency acceptable use and confidentiality agreement prior to the use of FDOE information technology resources. The agreement form is in Section 7.0 of this document. The completed form must be turned into the appropriate personnel liaison for inclusion in the employee's official personnel file.

5.3 Use of FDOE Information Technology Resources

- 5.3.1 Access to agency information technology resources is reserved for agency authorized users.
- 5.3.2 Workers must not use computer equipment that is not assigned to them without prior supervisory approval.

5.4 Personal Use of Information Technology Resources

5.4.1. It is recognized that, from time to time, occasions may arise wherein the limited use of information technology resources for a personal reason may be permitted and in the best interest of the Department and its users.

5.4.2 Personal use of technologies may be approved by supervisors as appropriate and within the following guidelines:

- a. The use of information technology resources for personal requirements shall not interfere with the users or any co-worker's job responsibilities or assigned tasks.
- b. The usage shall occur in a user's own time, e.g., during a break or lunch period, except as otherwise authorized.
- c. All such usage shall be kept to a minimum and not incur any measurable cost to the state, in use of paper, ink or wear and tear on the equipment. Note: Personal usage may result in reimbursement for costs associated with personal use.

5.4.3 Workers are responsible for complying with state, federal, and local laws and the Department's policies on technology use and resource security.

5.5 Access Authorization and Authentication

5.5.1 Agency computer users shall have unique user accounts.

5.5.2 Agency computer users shall be held accountable for their account activities.

5.5.3 User accounts shall be authenticated at a minimum by a user ID and password.

5.5.4 Agency computer users are responsible for safeguarding their passwords and other authentication methods.

5.5.5 Agency workers shall not share their agency accounts, passwords, personal identification

numbers, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes.

- 5.5.6 Agency workers shall immediately report suspected account compromises to their supervisor and to the FDOE Information Security Manager.
- 5.5.7 Agency workers shall immediately report lost security tokens, identification badges, or other devices used for identification and authentication purposes according to agency incident reporting procedures. (See the computer Security Incident Response Policy for additional information.)
- 5.5.8 Supervisors shall:
 - a. Approve the assignment of employee or user IDs for access to data;
 - b. Initiate access to other specialized applications;
 - c. Provide the Education Data Center with written requests to delete all IDs of terminated employees or other workforce members.
- 5.5.9 Supervisors shall also be responsible for ensuring that the Education Data Center and specialized application managers are notified when employees or other workforce members terminate from the Department by notifying the Personnel Office in an email.
- 5.5.10 FDOE Personnel Management shall notify the FDOE Helpdesk of all workforce terminations. The appropriate Education Data Center staff shall immediately disable all applicable IT resource user IDs and accesses. The Data Center staff shall notify the FDOE ISM of the action taken upon completion.

5.6 User Privacy

- 5.6.1 The agency shall be allowed to inspect any and all files stored on agency network or computer systems, including attached removable media.
- 5.6.2 FDOE shall be allowed to monitor the use of its information technology resources.
- 5.6.3 Use of FDOE information technology resources constitutes consent to monitoring activities whether or not a warning banner is displayed.

5.7 Public Records / Information

- 5.7.1 Any information generated through a computer, stored on disk, or electronically mailed is subject to all rules governing public records. (Public Records, Chapter 119, F.S.).
- 5.7.2 With few exceptions, information generated through a department computer, stored on any media, or sent or received electronically, such as email, is a public record. These records are subject to all laws governing the maintenance and disposal of public records. For further information, consult the Department's Public Records Policy.

5.8 Access to Information and Data

- 5.8.1 Users working with confidential information must follow the standards outlined in the Data Classification and Handling Policy.
- 5.8.2 Except as provided below, users must view only technology information or data they are authorized to view to do their job. (See definition for Need-to-know.)
- 5.8.3 Users who become aware of a suspected or actual information security breach must contact the FDOE Helpdesk and/or the Information Security Manager.

Personally Identifiable Student Records

- 5.8.4 Users who have access to personally identifiable student records shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), Section 1002.22 F.S., and Section 1008.39 F.S., and other applicable laws and regulations, as they relate to the release of student information.
- 5.8.5 Users shall not use access to student records information for personal gain. In no case shall personally identifiable information be released publicly.
- 5.8.6 Users are to refrain from viewing or printing personally identifiable information except to perform their assigned duties.
- 5.8.7 Users authorized to access personally identifiable information shall execute a separate acknowledgment indicating they are aware of additional provisions of applicable laws and

regulations. The form shall be provided by and kept on file by the business unit that owns or oversees the information.

People First Employee Data

- 5.8.8 The People First System enables employees to record time, attendance, leave, and personal information. Employees who use or have access to this information must use such information for legitimate business purposes only. Employees are prohibited from disclosing confidential information accessed in the system or from using the information for personal purposes or personal gain.
- 5.8.9 The “casual viewing” of employee data constitutes misuse of access, is not acceptable, and will not be tolerated. Database queries are performed by People First and the Department of Management Services on a regular basis to identify misuse of the People First System. Violators of this policy will be subject to disciplinary action, up to and including dismissal, and may be subject to criminal prosecution.

5.9 System and Network Activities

- 5.9.1 Only authorized IT staff are to connect network devices and/or microcomputers to the existing FDOE network.
- 5.9.2 Users shall not connect any device to the FDOE internal network without the knowledge and written authorization of the Data Center Director and the Information Security Manager.

Note: This FDOEs not include the FDOE wireless guest network. The FDOE guest wireless network will allow any wireless device to connect to the internet.
- 5.9.3 Only authorized users may create and publish websites. For further information contact the FDOE Communications Office.

5.10 Copyright

- 5.10.1 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which there is no active license is strictly prohibited.
- 5.10.2 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The Department’s General Counsel shall be consulted prior to export of any material that is in question.

5.11 Prohibited Uses

- 5.11.1 Users shall not introduce malicious programs or tools into the network or server environment (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- 5.11.2 Using any computing asset to actively engage in procuring, viewing, or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user’s local jurisdiction is prohibited.
- 5.11.3 Making fraudulent offers of products, items, or services originating from any State of Florida account is prohibited.
- 5.11.4 Users shall not engage in port scanning activities of any kind unless preapproved in writing by the FDOE Information Security Manager and Chief Information Officer.
- 5.11.5 Users shall not circumvent user authentication or security of any host, network, or account.
- 5.11.6 Users shall not participate in disruptions of network communication, unless this activity is scheduled and is a part of the user’s normal job/duty, which includes but is not limited to:
 - a. Introducing any process resulting in a cyber-attack or denial of service attack.
 - b. Executing any form of network monitoring/sniffing that consumes or absorbs bandwidth or increases traffic.
 - c. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable a user’s computing session, via any means, locally or via the internet/intranet/extranet.
- 5.11.7 Effecting security breaches which include but are not limited to, accessing data to which the user is not an intended recipient or logging into a server or account that the user is not

expressly authorized to access is prohibited, unless these duties are within the scope of regular duties.

- 5.11.8 Agency computer users shall not attempt to access information technology resources for which they do not have authorization or explicit consent.
- 5.11.9 Users shall not provide access to confidential or proprietary information to unauthorized individuals.
- 5.11.10 FDOE IT resources shall not be used for any purpose which violates state or federal laws or rules.
- 5.11.11 FDOE IT resources shall not be used for personal profit, benefit or gain, or to promote or benefit an individual or private business.
- 5.11.12 FDOE IT resources shall not be used to access, create, store, or transmit offensive, indecent, or obscene material.
- 5.11.13 FDOE IT resources shall not be used to access applications, software, websites or other systems associated with QQ, TikTok, WeChat, VKontakte and Kaspersky.
- 5.11.14 Agency computer users shall not use FDOE IT resources to engage in activities that may harass, threaten, or abuse others.
- 5.11.15 FDOE IT resources shall not be used for political campaigning or unauthorized fund raising.
- 5.11.16 Agency computer users shall not circumvent department computer security measures.
- 5.11.17 FDOE IT resources shall not be used for any activity that adversely affects the availability, confidentiality, or integrity of information

5.12 Electronic Data Communications

Transmitting by email, instant message, chat, or any other electronic means, or viewing on the Internet any inappropriate material is strictly prohibited. (See definition for Inappropriate material.)

Email

Messages sent as electronic mail (email) shall meet the quality standards for distribution and display as if they were tangible documents or instruments. When sending messages, users shall abide by all security restrictions on information to which they have access, regardless of whether the email is accessed from within the Department or through remote access. Electronic mail shall be used for Department-related purposes and not for personal use or gain.

- 5.12.1 Agency computer users shall follow agency established guidelines for acceptable use of email resources.
- 5.12.2 Email containing confidential information must be encrypted or transmitted via an approved FDOE solution. (Contact the FDOE ISM for information regarding secure mail.)
- 5.12.3 Inappropriate use of agency email includes, but is not limited to, the following:
 - a. distribution of malware;
 - b. forging email headers;
 - c. propagating “chain” letters; and
 - d. forwarding or auto-forwarding agency email to a non-agency email address for making a duplicate copy accessible outside the FDOE security boundaries.
- 5.12.4 If a user receives an email containing inappropriate material, the user must take the following action:
 - a. If the sender of the email is personally known to the user, the user must:
 - Refrain from replying, forwarding, or deleting the email;
 - Notify the sender by phone or in a separate email to cease sending such materials since receipt or transmission of such material is inconsistent with Department policy; and
 - Inform his or her supervisor of receipt of the inappropriate email.
 - b. If the sender of an inappropriate email is not known by the user, the user must:
 - Refrain from replying, forwarding, or deleting the email;
 - Inform his or her supervisor immediately that an inappropriate email has been received; and

- Follow the supervisor's instructions on the deletion or removal of offensive information.

Internet

Internet access and associated resources shall be used by workers to assist and enhance job productivity as it relates to Department business. These resources shall be used for Department-related purposes and not in any manner that will not result in direct or indirect benefits to the Florida Department of Education. (For exception see section 5.4 – Personal Use of Information Technology Resources.)

- 5.12.5 Agency computer users shall follow agency-established guidelines for acceptable use of Internet resources.
- 5.12.6 The Internet is not to be used to conduct any activities, which would be illegal under federal, state, or local laws, or would be otherwise prohibited under rules in the Florida Administrative Code.
- 5.12.7 Inappropriate use of the Internet includes non-work-related access to the following:
 - a. chat rooms, political groups, singles clubs, or dating services;
 - b. material relating to gambling, weapons, illegal drugs, illegal drug paraphernalia, or violence;
 - c. Applications, software, websites or other systems associated with QQ, TikTok, WeChat, VKontakte or Kaspersky.
 - d. hacker websites/software; and
 - e. pornography.

Instant Messaging / Chat

- 5.12.8 FDOE only authorized FDOE Instant Messaging (Microsoft Teams) that archives messages for public records to use systems connected to the FDOE network.

Use of Personal Text Messaging

- 5.12.9 The department prohibits each employee from conducting agency business via personal text messaging or other means of written communications that FDOE does not archive for public records. This would include but not be limited to short message service (SMS), instant messaging, cell phone texting, other similar technology, social media (e.g., Facebook, Twitter, etc.), or personal e-mail. See definitions for text messaging, SMS, and social media.
- 5.12.10 If a department employee receives a message related to agency business via personal text messaging, the employee should immediately inform the sender of this policy, and demand that future communications be sent via approved methods (i.e., the employee's fIFDOE.org email address or telephone).
- 5.12.11 The employee shall also forward the improper communication to their fIFDOE.org email address to ensure that the record is properly retained.
- 5.12.12 Any known or suspected violation(s) of this policy should immediately be reported to management for investigation. Violations may result in discipline up to and including dismissal.
- 5.12.13 The Department understands that an occasion may arise where employees may need to communicate with each other via personal text messaging. Such communication is permissible under this policy provided that the message is transitory in nature. See definition for transitory.
- 5.12.14 There is no prohibition against Department employees communicating via text messaging, social media, or personal e-mail provided that the communication is in no way related to agency business.

5.13 Non-FDOE Computers

- 5.13.1 Computers not issued by FDOE are not permitted to directly connect to the internal FDOE internal network. See section 5.30 for exceptions.

5.14 Software

- 5.14.1 All software on computers must be licensed. Workers are responsible for using software in accordance with licensing agreements. Users must observe copyright restrictions held

by the Department or State. Workers who use or have access to software are responsible for knowing and complying with all applicable terms and conditions regarding its use.

- 5.14.2 Users must not make or distribute unauthorized copies of software. Modifications cannot be made to the software that is not authorized by the copyright holder. A copyright legend or notice shall not be removed from the software or any of its documentation.
- 5.14.3 Commercial microcomputer software purchased by FDOE is authorized for FDOE use only. Making copies of FDOE-purchased software for personal use is illegal and prohibited.
- 5.14.4 Users must contact the Education Data Center when questions arise as to terms, conditions, and restrictions on information technology resources and databases.
- 5.14.5 Even though an employee has terminated their employment with the Department, the former employee can be personally subject to legal action by infringing upon copyright or intellectual property rights.
- 5.14.6 Beta software is not supported, nor can it be installed on production computers without written approval from the Data Center Director. If there is a need to test beta software for a project, the testing shall be done in an FDOE-approved test environment.
- 5.14.7 Applications known to promote adware are not allowed on the desktop.
- 5.14.8 Users shall not install personally owned software on FDOE-owned information technology resources. See Section 5.30 for exceptions.
- 5.14.9 Only software with valid licensing shall be installed on FDOE-owned IT resources.
- 5.14.10 Users shall not install any program files (executable, shareware, freeware), or personal files on their network home directory or on any network drive.
- 5.14.11 Users shall not install software on their assigned computing device. Authorized IT staff are to install software necessary to perform job duties.
- 5.14.12 No software that promotes or enables peer-to-peer file sharing functionality will be allowed on any computer connected to the FDOE network.

5.15 Hardware

- 5.15.1 Hardware and related equipment acquired by the State or Department shall be used exclusively for Department business.
- 5.15.2 Users shall not use any FDOE-issued hardware or related equipment for private business or personal use. (For exceptions, see section 5.4 – Personal Use of Information Technology Resources.)
- 5.15.3 Users shall not use FDOE-issued hardware to access information not related to their assigned responsibilities, and it shall not be used for recreational purposes such as computer games, accessing Internet sites that are not work related, or for production of printed materials for other than Department business. (For exceptions, see section 5.4 – Personal Use of Information Technology Resources.)
- 5.15.4 Transfer of IT hardware requires the user to complete a Property Transfer Form. For additional information contact the FDOE's Bureau of General Services or the appropriate property Custodian.

5.16 User Data

- 5.16.1 Only user data saved in the user's network directories on the LAN (Local Area Network) file servers will be backed up by FDOE IT staff. The user's network home directory is for the storage of data files that are created by application programs on the user's desktop computer.
- 5.16.2 Users are responsible for ensuring their data is stored on network drives or to ensure their data is backed up in a manner that the data can be recovered in the case of theft, loss, or system crash.
- 5.16.3 Users shall not use free online (Cloud Computing) storage solutions to store FDOE data. Only entities that are under contractual agreement with FDOE shall be used to store FDOE data and information. See section 5.30 for exceptions.

5.17 Wireless

- 5.17.1 No end-user at any time is authorized to set up a wireless access point on FDOE premises. The installation of wireless connectivity is to be under the control of FDOE IT staff with the knowledge and approval of the CIO and ISM. To ensure security, all unauthorized wireless access points will be shut down immediately upon discovery.
- 5.17.2 Users shall not run their laptops in wireless ad-hoc mode. This potentially allows other users to connect to the laptop in a peer-to-peer connection.
- 5.17.3 FDOE supports public and private wireless connectivity. Users wishing to utilize FDOE wireless access must follow the standards outlined in the FDOE Wireless (Wi-Fi) Acceptable Use Policy.

5.18 Network

- 5.18.1 Monitoring, sniffing, and related security activities shall be performed only by workers based on job duties and responsibilities when given explicit consent.

5.19 Virtual Private Network (VPN Access)

- 5.19.1 Users may remotely connect computing devices directly to the FDOE network only through DFOE-approved, secured remote access methods.
- 5.19.2 Only DFOE-issued or FDOE-managed computing devices are allowed to remotely connect to the FDOE network.
- 5.19.3 VPN Access will only be granted for legitimate FDOE business.
- 5.19.4 Users granted VPN access shall not allow others to use their assigned VPN connection.
- 5.19.5 Computing devices shall enable an FDOE-approved personal firewall (where technology permits) when connecting via VPN to the GDOE network.
- 5.19.6 A VPN session shall be automatically terminated after a pre-determined length of inactivity. No automated processes shall be used to keep the VPN connection open absent user interaction.
- 5.19.7 Users shall not store passwords in a non-FDOE-approved software application, including web browsers, at any time.
- 5.19.8 FDOE security and privacy policies must always be followed when using or connecting to FDOE Information Technology resources.

5.20 Desktop Security

- 5.20.1 Users shall NOT remove and/or in any way attempt to disable any IT security software installed and/or configured by the FDOE IT staff. This can include, but is not limited to, the following: anti-virus software, anti-spyware software, password enabled screen-saver utility, personal firewall, ECM agent, and/or host-based IDS.

5.21 Anti-Virus / Anti-Spyware

- 5.21.1 Any PC-based computer or laptop that connects to the FDOE internal network shall have anti-virus and anti-spyware software installed and scheduled to run complete scans at regular intervals.
- 5.20.2 Any PC-based computer or laptop that connects to the FDOE internal network shall have anti-virus and anti-spyware software installed and running in the background to perform real-time scanning while the system is in use.
- 5.20.3 The anti-virus and anti-spyware software and signature files shall be kept up to date.
- 5.20.4 Unauthorized personnel shall not modify the configuration of FDOE provided anti-virus and anti-spyware protection software after installation.

5.22 Computer Lockdown

- 5.22.1 Users shall lock their workstation, or log out, whenever their workstation is unattended.
- 5.22.2 Screen savers on all operating system platforms (Windows XP, etc.) shall have passwords set to engage after 15 minutes or less of inactivity.
- 5.22.3 Authorization for applying a power on password (BIOS enabled passwords) shall come from the Data Center Director.

5.23 Dual Connectivity

- 5.23.1 Desktop computers are not permitted to have both a network interface card (NIC) and modem. This creates a potential security violation.
- 5.23.2 Laptops are NOT included in this standard. However, while laptops may have a NIC, with wireless and modem capabilities, they are not to be connected simultaneously. That is, a user is not to dial-in to an Internet service provider and at the same time be connected to the FDOE LAN.
- 5.23.3 Users shall not set up their computer or laptop to accept dial-in connectivity.

5.24 Laptops

- 5.23.1 Security mechanisms to protect both the physical asset (laptop) and the information contained by the laptop (data) are to be implemented and maintained.
- 5.23.2 New laptop purchases are to be purchased with approved security cable locks. Cable locks are to be purchased and put in use for all existing FDOE laptops.
- 5.23.3 Laptops used as workstations shall be secured with a cable lock or with a locked-down docking station.
- 5.23.4 All confidential or sensitive data stored on a FDOE laptop shall be encrypted with an approved encryption solution. Contact the FDOE ISM for further information.
- 5.23.5 The laptop user is responsible for ensuring all data stored on a FDOE laptop is backed up in a manner that the data can be recovered in the case of theft or system crash.
- 5.23.6 In the event that a laptop is lost or stolen, the user is to follow appropriate FDOE procedures. (See section 5.28 – Stolen or Missing Equipment.)

5.25 Mobile Devices

- 5.25.1 Users who wish to use their personal mobile devices for email and calendar synchronization with FDOE resources must follow the standards outlined in this Acceptable Use Policy.
- 5.25.2 Users with FDOE-issued mobile devices must follow the standards outlined in this Acceptable Use Policy.

5.26 Remote Management

- 5.26.1 Users are not to remove or disable the remote management client from their desktop. If problems seem to be related to the remote management client, then the FDOE IT staff, at their discretion, will disable the client or modify the configuration.
- 5.26.2 Remote management of a user's computer shall require the user's knowledge and explicit permission. This requirement will be waived in the event of a formal investigation with the written permission of the CIO or the Inspector General.

5.27 Maintenance

- 5.27.1 Workstations and laptops shall be maintained with the latest software patches, anti-virus and anti-spyware signatures, updates, and software rollouts. In order to facilitate this process, users shall observe the procedures outlined by their respective data center regarding information technology resource maintenance schedules.

5.28 Stolen or Missing Equipment

- 5.28.1 Users are responsible for securing State property. Users who believe their State or personal property has been stolen should immediately report the suspected theft to the Office of the Inspector General at (850) 245- 0403. The suspected theft also should be reported to the users' immediate supervisor and to the appropriate Property Custodian.
- 5.28.2 The FDOE Information Security Manager must be notified in the event of any suspected or actual loss or theft of a laptop, or any media (see definition for Media) that contained FDOE information or data.

5.29 Security Awareness Training

- 5.29.1 Users must annually participate in information security awareness training. Training is provided through an online portal and the link will be provided by the supervisor or

Information Security Team.

- 5.29.2 All new hires and new contractors must complete Information Security Awareness Training within 30 days of starting employment with FDOE. See Security Awareness Policy.

5.30 Enforcement

- 5.30.1 Violation of these standards may result in the agency taking disciplinary action appropriate to the violation, up to and including termination and/or criminal prosecution.

5.31 Exceptions

Use of Non-FDOE Computers

- 5.31.1 The use of non-FDOE computers and associated equipment in support of State-related work at the home or the workplace is discouraged; however, it may be authorized if properly certified. (Forms may be obtained from the FDOE Helpdesk or the Information Security Manager.)
- 5.31.2 FDOE is not responsible for non-FDOE computers damaged or needing repair as the result of State-related work.
- 5.31.3 Users shall certify that their non-FDOE computer meets or exceeds the FDOE security standards outlined below.
- a. The operating system shall have the latest patches applied. Any operating system no longer supported is not permitted to connect directly to the FDOE network. (For further information contact the FDOE ISM.)
 - b. Windows systems shall be running an up-to-date anti-virus and anti-spyware solution with up-to-date signature files.
 - c. Windows, Macintosh, and Linux systems shall run a personal firewall.
 - d. Windows, Macintosh, and Linux systems shall run a password enabled screen saver.
 - e. Windows, Macintosh, and Linux systems shall keep security patches and updates current.
 - f. No applications or Software associated with QQ, TikTok, WeChat, VKontakte or Kaspersky shall be installed on the device.
- 5.31.4 Computers not issued by FDOE shall not be allowed to connect directly to the FDOE internal network without approval. (Forms may be obtained from the FDOE Helpdesk or the Information Security Manager.)
- 5.31.5 Use of a non-FDOE computer must be approved by the Information Security Manager and the record of approval shall be maintained by the Information Security Manager.
- 5.31.6 At a minimum, approval for non-FDOE computers shall be renewed annually.
- 5.31.7 The computer owner is responsible for meeting all established FDOE standards for copyrighted software.
- 5.31.8 The individual owner is responsible for the maintenance and repair of non-FDOE computers.

Use of Free Cloud Computing Solutions for File Transfers

- 5.31.9 Use of cloud computing solutions (e.g., Dropbox, box, YouSendIt, SkyDrive, etc.) cannot be used at any time for restricted or confidential data or information. There are no exceptions to this standard.
- 5.31.10 The FDOE ISM must approve writing the use of cloud computing solutions for the transfer of public FDOE data that cannot be accommodated by FDOE's email solution. A help desk request must be initiated by the requestor for assistance with this need.

Use of Personally Owned Software

- 5.31.11 Personal software must be properly licensed, and the software owner must be able to demonstrate legitimate ownership.
- 5.31.12 Personal software must be for work purposes, not for desktop enhancements (e.g., screen saver applications, photo organizers, etc.). The Desktop Support and the ISM must approve the use of personal software.

6.0 Reference Documents:

Chapter 119, Florida Statutes

Section 282.318, Florida Statutes

Chapter 815, Florida Statutes
Section 1002.22, Florida Statutes
Section 1008.39, Florida Statutes
Chapter 60GG-2, Florida Administrative Code (F.A.C.)
Educational Rights and Privacy Act (FERPA)

7.0 Applicable Forms:

Appendix A: Acknowledgement of Compliance with Information Security Policies - The signed form is to be kept on file.

8.0 Department Contact:

Policy Owner Division/Section/Office Name:	Office of Technology and Information Services
Address	1144 Turlington Building
Telephone	850-245-0517
Help Desks FDOE Division Blind Services (DBS) Office of Early Learning (OEL) Division of Vocational Rehabilitation (VR)	850-245-9444/HelpDesk@fldoe.org 850-245-0360/DBS.HelpDesk@dbfs.fldoe.org 850-717-8600/HelpDesk@oel.myflorida.com Contact Local IT Technician through Fix-IT ticketing system
Information Security (Infosec) FDOE InfoSec Manager/Office DBS OEL VR	850-245-9506/850-245-0727/InfoSecTeam@fldoe.org 850-245-0337 850-717-8585/Information.Security@oel.myflorida.org 850-245-3305/VRITSecurity@vr.fldoe.org

Acceptable Use Policy

Acknowledgement of Compliance with Information Security Policies

I, _____, have read and understand all of the

(PRINTED OR TYPEWRITTEN NAME OF EMPLOYEE)

policies and procedures stated in this document, and I acknowledge that failure to comply with these policies and procedures may result in civil liability, disciplinary actions up to and including dismissal, or other sanctions.

Signature of Contractor

Date

Attachment I
Addendum Acknowledgment Form

Please complete and return this form with your proposal as applicable (Only if Addenda is issued).

ADDENDA ACKNOWLEDGMENT: The undersigned acknowledges the receipt of the following Addenda:

ADDENDUM NO. _____ DATED _____ ADDENDUM NO. _____ DATED _____

ADDENDUM NO. _____ DATED _____ ADDENDUM NO. _____ DATED _____

ADDENDUM NO. _____ DATED _____ ADDENDUM NO. _____ DATED _____

ADDENDUM NO. _____ DATED _____ ADDENDUM NO. _____ DATED _____