Early Learning Coalition of Broward County, Inc.

Governance Committee Meeting Agenda

6301 NW 5th Way, Suite 3400,
Fort Lauderdale, FL 33309

Thursday, January 12, 2017
3:00 pm

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

I.	**Call to Order**		Fabienne Fahnestock, Governance Chair
II.	**Roll Call**		
III.	**Agenda** a. Approve November 3, 2016 Minutes b. Approve April 20, 2016 Minute Revisions *(revisions requested at 11/3/16 meeting)*	**(Tab 1)** pg. 2 - 3 **(Tab 2)** pg. 4 - 6	Fabienne Fahnestock, Governance Chair
	c. Review and Approve IT Data Security Data Policy	**(Tab 3)** pg. 7 - 44	Hubert Cesar, IT Manager Jacob Jackson, General Counsel
IV.	**Unfinished Business** **New Business** **Matters from the Committee** **Matters from the Chair** **Public Comment** **Next Meeting: TBD** **Adjourn**		Leticia Strasser, COO

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

Early Learning Coalition of Broward County
Governance Committee Meeting Minutes
November 3, 2016 – 10:00 am
6301 NW 5th Way, Suite 3400, Fort Lauderdale, FL 33309

Members in Attendance: Mason Jackson, Fabienne Fahnestock

Members Absent: Barrington Russell, Laurie Sallarulo (optional)

Staff in Attendance: Leticia Strasser, Doreen Moskowitz, Irene Ramos

Others in Attendance: (from sign-in sheet) Jacob Jackson – General Legal Council

Item	,	Follow-up
Call to Order and Roll Call	Fabienne Fahnestock, Chair called Governance meeting to order at 9:20am. Roll call was made.	
Minutes	Fabienne requested a motion to approve the April 20, 2016 Meeting Minutes. Mason would like to see the revision to the Attendance Monitoring Procedure pointed out in the minutes and so the approval of minutes will be deferred.	
COOP	Leticia gave history of the COOP Plan August 2016 version indicating the editing made in red and added that these changes have been reviewed by Jacob Jackson Legal Council. Committee reviewed and provided corrective suggestions to the COOP to include consolidated statements to avoid conflicting issues and a visual for quick reference. Areas of needed revision were noted as: • Disaster Magnitude • Travel Reimbursement Policy • Board Member notification • Alternative Facilities	

	• Warning Conditions • Communications Chair • Designation of Authority • Mode of Communication and Storage of Data • Activation of COOP Substance of COOP should be defined to include any ongoing changes that can occur and that information should be reviewed and confirmed on an annual basis and a special reference to relocation entities. Committee members do want to see updated revisions made. OEL can make a suggestion on a good COOP policy to reference from.	
	Motion made by Mason to table the COOP and bring back in a more concise form. **Second** by Fabienne.	
New Business	IT policy is in review regarding the COOP process and will be brought to the committee in January 2017.	
Old Business	None	
	Next Governance meeting to be held on January 12, 2017 at 3pm.	
	Motion to adjourn made by Fabienne **Seconded** by Mason. Meeting adjourned at 10:24am	

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

PLACEHOLDER - FOR 4/20 REVISED MINUTES

PLACEHOLDER - FOR 4/20 REVISED MINUTES

PLACEHOLDER - FOR 4/20 REVISED MINUTES

Data/Systems Security Plan

Revision ~~March~~ December 2016

TABLE OF CONTENTS

ELC Policy Name: **Data Security and Systems Policy a~~A~~nd Procedure**
ELC Policy No.: **OPM___**
Approval Date: **Pending Board Approval**
Rev. Date(s): **12/16, 3/16, 9/14, 3/12**
COA Standards: **OPM___**

STATEMENT OF POLICY

As part of its mission, the Early Learning Coalition of Broward County, Inc. ("ELC") maintains computers, cell phones, computer systems and a network. These computing resources are intended for ELC-related purposes. For purposes of this policy and procedure, "S~~Data s~~ystem" shall mean all computing, network and web/cloud based resources including, but not limited to, the use of electronic mail, internet, intranet, web pages, video communication, cell phones, computer software, computer hardware and cloud/server based storage. If you have any questions regarding this policy, contact the ELC~~Coalition~~'s IT ~~Designee~~ Department for further information. It is the role of the ~~Coalition~~ ELC's IT ~~Designee~~ Department to ensure this policy is implemented effectively across the organization.

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

This policy cannot lay down rules to cover every possible situation. Instead, it expresses the ELC's philosophy and sets forth general principles to be applied in the use of ELC data systems. ELC expects its ELC staff to be mature professionals who understand that they are to use good judgment when it comes to using the ELC's data system. This policy is designed to simply lay out basic principles and premises of the use of the ELC's data system for the transaction of ELC business and otherwise.

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

PURPOSE OF POLICY

Security is highly important for the Early Learning Coalition of Broward County. For this reason the following policies are create ~~T~~to ensure that all personal identifying data, assessment data, and health data of all families and children served are guaranteed to be safe and confidential and release of data is in accordance with the guidance of Office of Early Learning ("OEL").

SCOPE OF THE POLICY

The following procedures apply to all employees of the ELC, contractors, vendors and their respective data systems that are:

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

Board Chair's Signature:_____ Date Signed:_____

STATEMENT OF PROCEDURE

Definition(s)

1. **Board** shall have the same meaning as it does in the ELC bylaws

2. **Breach of Security** shall mean an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data **breaches** may involve personal health information (PHI), personally identifiable information (PII), Protected personally identifiable information (PPII), trade secrets or intellectual property.

2. **Chair** shall have the same meaning as it does in the ELC bylaws

3. **Chief Executive Officer ("CEO")** shall have the same meaning as it does in the ELC bylaws

4. **Client** shall mean the intended recipients of the ELC and/or Florida's Office of Early Learning ("OEL") grant related activities or funding, including, but not limited to the ELC's Voluntary Pre-Kindergarten ("VPK") or School Readiness ("SR") programs and services such as children, parents and legal guardians.

5. **Confidential** ~~**and Sensitive Information**~~ shall mean record systems, specific records or individually identifiable data that by law are not subject to public disclosure pursuant to applicable federal and Florida statutes, codes and other regulations. When applicable, this definition or any reiteration of it covers all documents, papers, computer files, letters and all other notations of records or data that are designed by law as confidential, including but not limited to those items that may be considered proprietary information, intellectual property, or trade secrets belonging to the ELC, OEL or a third party. Furthermore, ~~this definition~~the term confidential covers the verbal conveyance of data or information that is confidential~~ or sensitive in nature~~.

6. **Contractor** shall mean those eligible licensed entities that contract directly with the ELC to provide School Readiness or Voluntary Pre-Kindergarten services and/or programs in accordance with Florida Statutes and provides monitoring, investigations and/or other oversight functions on behalf of the ELC to Service Providers. For purposes of this policy and procedure, the term **"Contractor"** shall have the same meaning as the term "**lead agency"** or **"sub-recipient"** in any statewide agreement(s) created by the Office of Early Learning, any other governing state agency or authority for the ELC, any applicable federal or Florida statutes, or within any contract or agreement with a third party concerning VPK or SR services.

7. **ELC** shall mean the Early Learning Coalition of Broward County, Inc. For purposes of this policy and procedure, the term **"Coalition"** shall have the same meaning as the term **"ELC"**.

8. **ELC staff** means those persons directly employed by the ELC.

9. **Member** shall have the same meaning as it does in the ELC bylaws.

10. **Personally Identifiable Information ("PII")** shall mean information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

11. **Protected Personally Identifiable Information ("PPII")** shall mean information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

12. **Public Records** shall mean any hard copy or electronic copies of records made or received by any public agency in the course of its official business. Records such as policies, minutes, files, accounts, program results, computer records, emails, Facebook and text messages are all available for inspection unless specifically exempted in state statute.

13. **Security Incident** shall mean a warning that there may be a threat to information or computer security. The warning could also be that a threat has already occurred. Threats or violations can be identified by unauthorized access to a system.

~~10~~1~~4~~3. **Service Providers** shall mean an eligible public school, private school, licensed or license-exempt child care entity that has provider agreement with the ELC and/or a Contractor to provide Voluntary Pre-Kindergarten ("VPK") or School Readiness ("SR") program services directly to children in Broward County in accordance with Florida Statutes. For purposes of this policy and procedure, the term **"Service Provider"** shall have the same meaning as the term **"Provider"** in any statewide agreement(s) for VPK and SR created by the Office of Early Learning ("OEL"), any other governing state agency for the ELC, any applicable federal or Florida statutes, or within any contract or agreement with a third party concerning VPK or SR services

~~11~~1~~5~~4. **Subcontractor** shall mean those **p**ersons or entities that have a contract with the ELC or a Contractor and are retained to perform either a portion or all of the SR and/or VPK program related services on behalf of the Contractor or ELC under those original contracts. For purposes of this definition, "SR and/or VPK program related work" shall mean services that would not fall under the definition of a **"Vendor"** such as instructional, client engagement, monitoring, and reporting. This definition shall also exclude those person or entities that deliver or perform professional services. For purposes of this definition, "professional services" shall mean accounting, finance, audit, legal or licensed healthcare related services.

1~~6~~5~~3~~. **Vendor** shall mean a dealer, distributor, merchant or seller who provides goods and services within business operations; provides similar goods or services to many different purchasers; operates

in a competitive environment; provides goods or services that are ancillary to the operation of the federal program; and is not subject to compliance requirements of the federal program. For purposes of this policy and procedure, the term **"Consultant"** shall have the same meaning as the term **"Vendor.**

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

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

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

USE OF ELC ~~'S DATA~~ SYSTEMS

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

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

To safeguard data and confidential information, ELC prohibits the use of personal data storage devices on the network in order to ensure conformity and that every employee is only using an ELC approved secure-encrypted flash drive. ELC staff are not allowed to use personal computers in order to access mission

critical servers/files systems and databases, but may be given secure access to the Internet via a secured guest ~~wifi~~Wi-Fi network, which does not allow users access to ELC's internal ~~in the main~~ network.

Electronic information created and/or communicated by an employee using electronic mail, word processing, utility programs, spread sheets, internet access, or any other ELC computing resource or data systems, will not generally be monitored by ELC. However, the following conditions should be noted:

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

2. The ELC also reserves the right, in its discretion, to review, monitor, audit, intercept, access and/or disclose any employee's electronic files and messages and usage and/or the hard drive, software or any other computing resource of any ELC employee for any lawful purpose including, but not limited to, ensuring that ELC resources are being used in compliance with applicable federal and Florida laws as well as in accordance with the ELC's policies and procedures.

3. ELC staff should not assume that electronic communication or data stored on in accordance with this policy and procedure are totally private and confidential and should take proper steps to transmit highly sensitive or personal information in other ways. ELC staff should not assume that ELC ~~data~~ systems are their personal property.

4. ELC staff must respect the confidentiality of other people's electronic communications and may not attempt to "hack" into other systems or other people's logins, or "crack" passwords, or breach computer or network security measures. ELC staff may not monitor electronic files or communications of other ELC staff or third parties except explicit direction of ELC staff~~personnel~~.

5. The ELC reserves the right to remove ELC ~~data~~ system privileges from an employee.

6. The ELC ~~data~~ systems are not to be used for personal commercial purposes or for personal, financial or other gain.

7. No employee will knowingly create access to ELC ~~-~~'s ~~data~~ systems in such a way to bypass ELC's security systems.

8. No employee will use ELC ~~data~~ systems for illegal activities.

9. All ELC staff will do their best to ensure all software or data is virus free before it is installed or loaded on the ELC's data ~~systems~~network. Any detection of a software or hardware virus or suspicion that a file may contain a software or hardware virus ~~will~~ must~~should~~ be reported immediately to the ~~ELC Data and Technology Coordinator~~ELC's~~Coalition~~ IT ~~Designee~~Department. ELC staff will be trained on a regular to make them aware of data security threats.

10. Violation of this policy and/or violations of relevant laws, statutes and ordinances may result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

11. Contractors and Vendors must sign a non-disclosure agreement protecting any confidential data to which the ~~-~~Contractor or Vendor requires access.

ELECTRONIC TRANSMISSION ~~& CONFIDENTIAL DATA POLICY & PROCEDURES~~

Transmission Procedures

The Coalition and its Contractors and its Vendors must safeguard private and confidential data such as names, addresses, social security numbers, and federal employment numbers. Unencrypted transfer of private and confidential information by e-mail or mobile devices (flash drives, thumb drives, cell phones or laptops) is prohibited. This prohibition applies to submissions to the Office of Early Learning ("OEL"), Department of Education ("DOE"), as well as transmissions among contractors and sub-recipients. All transmission of confidential data must be secured. The ELC's ~~Coalition~~ IT Department ~~Designee~~ strongly encourages staff to transmit confidential data via OEL SharePoint site or a secure File Transfer Protocol ("FTP") site. The ELC currently complies with requirements for restrictions on access to sensitive or confidential data as described in OEL's IT Policy and Program Guidance ~~101.02~~.

Examples of secure transfer of confidential data include but are limited to the following:

- Encryption of ~~-~~a file with a program ~~such as PGP or MySecret~~.
- The u~~U~~se of last names plus the last four digits of social security numbers.
- Fax only if the transmission is to a secure location and picked up immediately.
- Ensure that sensitive paperwork is secured and not in view of unauthorized persons~~.~~
- Transmit data behind a firewall.
- Transmit data via secure FTP

The following definitions and more information can be found in the applicable OEL p~~P~~rogram g~~G~~uidance regarding ~~101.02, r~~Records c~~C~~onfidentiality:

Acceptable Use of Information Resources

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

Information Resources Classification

All information resources (including data and systems) shall be identified, categorized and protected according to their level of confidentiality ~~and business "need to know"~~. All files should be stored and filed appropriately on the ~~main drive of the~~ ELC~~Coalition~~ s~~S~~erver (whether it is a physical or web/cloud based server).

Security Training and Awareness

The ELC~~Coalition~~'s information technology and security policies, procedures, and protocols shall be communicated to all ~~employees~~ELC staff, and shall be available for reference. Any c~~C~~hanges to those information technology and security policies, procedures, and protocols will be discussed at ELC ~~Coalition~~ staff meetings.

Incident Reporting

ELC~~Coalition~~ staff, Contractor, Vendors, Service Providers ~~personnel~~ and Subcontractors are required to report any suspected security incidents, unauthorized disclosures, security breaches or any security incident in accordance with the ELC's Incident Reporting Policy and Procedure. Incident reports should be reported and forwarded to the ELC~~Coalition~~'s IT Department ~~Designee~~ ~~system administrator~~immediately. The ELC is required to report any security breach or security incident to OEL in writing within 24 hours after learning of a security breach or incident.

Additionally, written notification to OEL must identify the following:

1. The nature of the unauthorized use or disclosure
2. The confidential information used or disclosed
3. Who made the unauthorized use or received the unauthorized disclosure
4. What the ELC has done or shall do to mitigate any harmful impact of the unauthorized use or disclosure and;

~~1.~~5. What corrective action the ELC has taken or shall take to prevent similar future unauthorized use or disclosure incidents.

Incident Response

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

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

~~**Security System Plans**~~

~~The Coalition's computer system shall contain a firewall.~~

Monitoring the Adequacy of System Performance and Hardware

The ELC~~Coalition~~ shall periodically monitor the appropriateness of access privileges assigned to users of certain systems; monitoring system hardware and periodically reviewing the appropriateness of access privileges assigned to users of certain systems; monitoring system hardware performance and capacity-related issues; and ensuring appropriate backup procedures and disaster recovery plans are in place.

Contingency Planning

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

Access Control

Access to the Coalition's ~~data~~ systems ~~information resources~~ shall be limited to those that need them to perform their job duties. ~~The principle of least privilege shall be applied to the allocation of access rights.~~ Procedures and protocols are in place to address and document the tasks that activate access to any production systems for ELC~~incoming~~ s~~s~~taff~~-~~, ~~or~~ C~~c~~ontractors or Vendors and to deactivate/remove access to all production systems for outgoing or transferring ~~employees~~ELC staff, ~~or~~ C~~c~~ontractors or Vendors which are in compliance with OEL's IT p~~P~~olicy regarding ~~5.05.02.16,~~ p~~P~~ersonnel s~~S~~ecurity. These include, but are not limited to, the following:

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

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

Identification and Authentication

Access to ~~the~~ ELC~~'s data~~~~Coalition information~~ systems shall be ~~only~~ granted to identified and authenticated users only.

Antivirus

This policy is in place so that the ELC~~Coalition~~ and its C~~c~~ontractor may verify that all computer systems are protected with antivirus and anti-malware software and that techniques are employed for avoiding viruses.~~Standard software and procedures shall be implemented to minimize the impact of computer viruses on the ELCCoalition's data systemsinformation resources.~~

Physical and Environmental Security

Automated information systems and facilities require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of ELC staff~~personnel~~. c~~C~~omputer systems, facilities, confidential records, personally identifiable information

(PII), protected personally identifiable information (PPII) and ~~tape~~ disk storage areas shall be protected from theft alteration, damage by fire, dust water, power loss and other contaminants and unauthorized disruption of operation.

Change Control

All security changes made to ~~the~~ any ~~–~~ ELC~~Coalition's data~~information~~ systems shall be made in a controlled and coordinated fashion to preserve the confidentiality, integrity and availability of the system.

Backup and Recovery

Recoverable backups shall be maintained for all critical systems at the ELC.~~th~~~~Coalition resource~~e ELC's ~~data systems~~s~~.~~

Patch Management and System Updates

The ELC ~~data s~~~~S~~ystems are to be maintained with updated security patches.

Server Security

Servers shall be made secure before placing them into the ~~Coalition~~ ELC's operational environment and security shall be maintained throughout their lifecycle.

Mobile Computing

Security c~~C~~ontrols shall be implemented to mitigate the increase risks posed by the use of laptops and other mobile devic~~es~~es outside of the ELC's~~Coalition~~ main office or site of operation~~office~~.

Network Security

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

Remote Access

Security controls shall be implemented to mitigate increased risks posed by allowing remote connectivity ~~into the ELC's data systems~~Coalition network to the ELC's internal network.~~.~~

Electronic Mail

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

Database Security

Information shall remain consistent, complete and accurate.

Media Management

Electronic m~~M~~edia shall be handled, stored and disposed of properly in order to protect the confidentiality of the ELC ~~data.Coalition data stored upon it~~.

Password Management

Passwords are an important aspect of the ELC's computer security. The ~~Coalition~~ ELC shall protect access to its ~~data~~ systems ~~information resources~~ by ensuring that any passwords used for authentication are properly assigned and protected. The ELC ~~Coalition s~~Staff shall also comply with requirements for passwords described in ~~OEL's IT Security Manual~~ the U~~u~~ser ~~access~~Account M~~m~~anagement P~~p~~rocedures as contained in this policy.~~.~~

Information Technology Asset Management

All information technology assets shall be tracked and managed to ensure that they are not lost or misused.

CONFIDENTIALITY

Statement

~~Employees~~ELC staff shall ensure confidentiality and privacy regarding history, records and any discussions relating to the Clients ~~people~~ who the ELC~~Coalition~~ or its Contractor, S~~s~~ubcontractors, or Vendors may~~s~~ serve. The very fact that a Client~~n individual~~ is served by the ~~Coalition~~ ELC or its Contractor, Subcontractors, or Vendors ~~subcontracts~~ shall be kept private or confidential unless~~;~~ disclosure is ~~can be~~ made ~~only~~ under for~~specified conditions, for~~ reasons relating to law enforcement, a court order, ~~and~~ fulfillment of a statutory requirement, ~~or~~ fulfillment of the ELC's~~our~~ mission that does not violate applicable law, or upon signed release by the Client~~said individual~~. ~~Employees~~ELC staff shall not disclose any information about a Client~~person~~, including whether that Client ~~person~~ is served by the ~~Coalition~~ ELC or its Contractor, Subcontractors, or Vendors ~~subcontracts,~~ to anyone outside of the ELC~~is organization~~, without prior approval of the Chief Executive Officer or other persons authorized by the Chief Executive Officer, if the CEO is so authorized to make said disclosure pursuant to applicable federal and Florida law or in accordance with ELC's policies, procedures and bylaws.

The principle of confidentiality shall be maintained in all programs, functions and activities. ~~Employees~~ELC staff shall not discuss any C~~c~~lient of the ELC ~~Coalition or subcontracts~~ with any unauthorized ~~individuals~~third party~~,~~ at any time, whether on or off duty. Confidentiality shall be maintained regardless of separation or termination of employment.

Maintenance ~~Pr~~rocedures

1. The ELC~~Coalition~~, i~~ and i~~ts Contractors, Subcontractors, and/or Vendors who receive early learning records in order to carry out official functions must protect~~s~~ the data in a manner that will not permit the personal identification of a Client ~~children or their parents~~ by persons other than those authorized to receive the records;

~~2.~~ The Contractors, Subcontractors, and/or Vendors ~~Subcontractors~~ of the ELC~~Coalition~~ shall have documented procedures to maintain confidentiality of early childhood and other confidential records consistent with this policy if said parties handle confidential information on behalf of the ELC;

~~3.~~

~~4. Requests for review of public documents shall be submitted in writing to the Chief Executive Officer. The Chief Executive Officer will review any documents before releasing them, to ensure no client data or other confidential data is disclosed.~~

~~5.~~**2.**

~~Compliance and Monitoringnfidentiality Procedures~~COMPLIANCE AND MONITORING

1. The ELC~~Coalition, and all of~~ its officers, ~~employees~~ELC staff, interns, volunteers, Members, agents, Contractors, Subcontractors, Service Providers and Vendors ~~and agents~~ shall comply with the applicable confidentiality provisions set forth in ~~Section 39.0132, 39.202, and 39.814, the~~ Florida Statutes ~~, and in any subsequent amendments to any of these statutes,~~ and shall not release any information regarding any of the~~-~~ ELC's Clients~~children in the child care/voluntary pre-kindergarten arrangements, or the family of children in the child care/voluntary pre-kindergarten arrangements~~, except as specifically authorized by Florida~~these~~ statutes. Failure to abide by the confidentiality requirements as set forth in those applicable Florida~~of these~~ statutes may constitute~~s~~ a criminal offense ~~as set forth in Section 39.205, Florida Statutes~~. The Coalition and all of its officers, ~~employees~~ELC staff, interns, volunteers, ~~and~~ agents, Contractors, Subcontractors, Vendors and Service Providers ~~-~~shall comply with applicable federal and Florida~~-~~ statutes, codes and other regulation as it concerns ~~Section 1002.97, as it relates the~~to records of children participating in ~~the~~ S~~s~~chool R~~r~~eadiness ("SR") ~~program~~ and ~~Section 1002.72, Florida Statutes as it relates to the~~ Voluntary Pre-kindergarten Education (VPK) Program~~s~~.

2. Monitoring by the ELC ~~results~~ will ensure that the ELC~~Coalition~~'s Contractors~~sub-recipient~~, Subcontractors, Service Providers and Vendors ~~s and their subcontractors~~ are in compliance with the following:

- Confidentiality provisions and the record retention requirements as set forth in ~~of Sections 119.01 and 1002.97, and 1002.72,~~ Florida and federal s~~S~~tatutes, where applicable.
- All data security measures of the Health Insurance Portability and Accountability Act ("HIPA~~P~~A").

3. Contractors, Subcontractors, Vendors and Service Providers~~Sub-recipients~~ of the Coalition shall ensure compliance with the following:

    - Shall not use or disclose any information concerning a Client ~~recipient of services under this Contract~~ for any purpose not in conformity with state and federal law or regulations except upon written consent of the Client ~~recipient, or his or her responsible parent or guardian~~ when authorized by law.

    - Shall comply with the Computer-Related Crimes Act, Chapter 815, Florida Statutes and ~~-~~shall demonstrate due diligence in safeguarding the Coalition's information resources by establishing policies and procedures for information systems security that contain criteria and standards as set forth in ~~F~~OEL's p~~P~~olicies and procedures~~y~~.

USER ACCOUNT MANAGEMENT PROCEDURES

It is the policy of the ELC to ensure user accounts utilized by ~~for employees~~ELC staff are standardized in order to minimize the potential exposure of the ELC ~~to damages~~, which may result from unauthorized user account access. This includes the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical ELC systems, and other unforeseen damages. As a result, the following procedures will be followed:

1. All ~~ELC employees~~ELC staff must read and sign the **Memorandum of Understanding ("MOU") and Data Security Agreement,** ~~(~~attached hereto as **Exhibit A** and hereby made a part of this policy and procedure,~~)~~ on an annual basis~~ly~~.

2. User accounts and passwords are the initial line of defense in network security. The Chief ~~Financial~~ Administrative Officer must approve the creation/change of account(s) for ~~employees~~ELC staff by completing the **System User Account Form** attached hereto as ~~(~~**Exhibit B** and by reference made part of this policy and procedure. ~~The)~~ The **System User Account Form** shall be submitted ~~and submitting it~~ to the ~~Coalition~~ IT Department ~~Designee ELC Vendor~~ for processing. ~~Employees~~ELC staff are granted the necessary privileges based on their account settings (f~~F~~iscal, p~~P~~rogram o~~O~~perations and a~~A~~dministration) to access files on the network server to accomplish day-to-day work.

3. Computer network passwords and user names are provided to ~~employees~~ELC staff to prevent unauthorized access to a computer. New users must change their password at their initial logon. Passwords are required to be at least eight (8) characters in length, and contain characters from three of the following four categories: English uppercase, English lowercase characters, Base 10 digits (0 through 9) and Non-alphabetic characters. Passwords to the ELC network are set to automatically expire every 60 days and prompt ELC users to automatically change/reset their passwords. Passwords cannot be reused for at least six (6) changes. ELC users should not reveal their password to anyone.

4. ~~ELC Employees~~ELC staff shall understand their responsibility for safeguarding user names and passwords, and immediately notify their supervisor and/or the Coalition IT Department~~Designee~~~~Information Officer~~ if they suspect that a password or the system credential has been compromised.

5. All user accounts are automatically set to lockout after three (3) unsuccessful/invalid login attend. Lockout account can only be reset manually by the ~~Coalition~~ELC's IT Department~~Designee..IT/Data Manager.~~ This policy will help prevent attackers from guessing users' passwords and it decreases the likelihood of successful attacks on the networks.

6. All workstations are set to automatically lockout (screen saver mode) after twenty minutes of inactivity timeout. The computer lockout is password protected by the user account. ~~Employees~~ELC staff are recommended to log off from the workstation when leaving the work area. Workstations should not be shut down overnight.

7. When an employee is transferred or employment is terminated, the user network account will be changed or deactivated immediately. The Accounting and Human Resources Manager will notify the ~~Coalition~~ELC's IT department ~~Designee~~ ~~IT/Data manager~~via email or written documentation (i.e. **System User Account Form)** on the day of transfers or termination of employment that require changes to ~~the~~ his/her user account.

Security Management/Access Control

The ELC is committed to protect and safeguard all data and electronic information systems from unauthorized use. All ~~employees~~ELC staff are assigned a user account and grant the necessary privileges based on their account settings to access the network and perform their job function.

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

1. Security measures are implemented by only granting specific access privileges to users required to perform their job duties based on the **System User Account Form** request.

2. Data folders are safeguard and can only be accessible based on access privileges

3. Regularly review records of system and security activity such as audit logs and access activity reports. ~~Coalition~~ELC's~~le~~ IT ~~Designee~~Department will perform desktop audit.

4. Regularly review VPN remote access audit log.

5. ~~Coalition~~ELC's IT ~~Designee~~Department ~~IT/Data Manager~~ will maintain a listing of ~~employees~~ELC staff who have been granted access, and will periodically review access permissions granted.

6. ~~Coalition~~ELC's IT ~~Designee~~Department ~~IT/Data Manager~~ will ensure that those granted access to data system have an approved Level II background screening and have received information security training in accordance with ELC protocols.

Security Training and Awareness

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

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

1. Data~~Information~~ security training and awareness will be provided to all new ELC staff by the ELC's ~~Coalition~~ IT ~~Designee~~Department ~~Information Systems Security Officer~~ covering this ~~e entire ELC computing resources~~ policy and procedure. Training to new ELC staff must be completed within ~~within~~ 30 days of new employment.

2. All ELC ~~information~~ users must complete an annual data security ~~information~~ training program provided by the Information Systems Security Officer to refresh their knowledge of data~~information~~ security. In addition, all ELC ~~information users~~ Staff must annually complete the Florida's Department of Children and Families ("DCF") O~~o~~nline Security Awareness Training.

3. All ELC ~~information users~~ Staff must sign an annual agreement that they understand the ELC's data ~~information~~ security policies and procedures within the ELC's computing resources policy and that they will abide by them. See Exhibit C**, Information Security Training Acknowledgement Form** ~~(~~attached hereto as **Exhibit C** and by reference made a part of this policy and procedure**.**~~).~~

Electronic Mail

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

While not an exhaustive list, the following are appropriate uses of electronic mail by individuals covered by this policy and procedure:

1. Electronic mail that is related to ELC business

2. Use related to administrative and other support activities of ELC. While not an exhaustive list, Tthe examples below regarding following the uses of electronic mail by individuals covered by this policy are considered inappropriate and unacceptable. In general, electronic mail should not be used for the initiation or retransmission of:

   - Chain mail that misuses or disrupts resources (e.g., electronic mail sent repeatedly from user to user, with requests to send to others);

   - Harassing or hate mail (e.g., any threatening or abusive electronic mail sent to individuals or organizations that violates ELC rules and regulations and this policy);

   - Virus hoaxes;

   - Spamming or electronic mail bombing attacks (e.g., international electronic mail transmissions that disrupt electronic mail service);

   - Sending or forwarding junk mail (e.g., unsolicited electronic mail that is not related to ELC business and which is sent without a reasonable expectation that the recipient would welcome receiving it);

   - Any actions that defraud another or misrepresent or fail to accurately identify the sender;

   - Sending copies of documents in violation of copyright laws;

   - Inclusion of the work of others into electronic mail communications in violation of copyright laws;
   - Capture and "opening" electronic mail except as required in order for authorized employeesELC staff to diagnose and correct delivery problems or as otherwise allowed by this policy;

   - Use of electronic mail to harass, intimidate or defame others or to interfere with the ability of others to conduct ELC business;

   - Use of electronic mail systems for any purpose restricted or prohibited by law, statute, ordinance or regulations;

- "Spoofing," (e.g., constructing an electronic mail communication so that it appears to be from someone else);

- "Snooping," (e.g., obtaining access to the files or electronic mail of others for purpose of satisfying idle curiosity);

- Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmission without proper authorization;

- Electronic mail or communications that attempt to hide the identity of the sender, or represent the sender as someone else from another entity; and

- Any other electronic communication that violates this policy, ELC Employee Handbook, or any other law, statute, regulation or ordinance.

Data Backup

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

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

Software:

Recognized industry approved software isare used to backup all ELC data on a nightly basis. Both software can be used to restore data in of an emergency.Any customized software that may be developed by our current data backup vendor maybe be is currently utilized to backup to, restore from, and verify data on secure off-site location.

Schedule:

An automatic full data backup using zip data is performed online daily and saved to a secure off-site location. A local external nNetwork aAttached sStorage devicedrive is also used to generate a data backup locally. The CoalitionELC's IT DesigneeDepartment IT/Data Manager monitors the success of these backups on a daily n ongoing basis and periodically reviews/updates to policy and processes for changes in operations, identifies important data files, periodically performs a restore testing and restore of databackup files, reviews backups and performs regular backups.

Media Devices/Physical/System/Data Security

It is the policy of ELC to ensure the protection of confidential data. The purpose of this specific procedure~~olicy~~ is to establish guidelines, procedures and requirements to ensure the appropriate protection of ELC~~'s data~~information systems. In doing so, the following steps must be implemented:

1. ~~Coalition~~ELC's IT Department~~Designee IT/Data Manager~~ is required to established appropriate user privileges, monitor access control logs and similar security actions for the systems he/she ~~administers~~ administers.

2. Computer resources and equipment must be stored in secure locations (server room, wiring closets, etc.) with restricted access.
~~4.~~
3. If the ELC~~coalition~~ determines that an item of grant-purchased property is no longer needed or required by the ~~ELC, coalition~~ its ~~or its~~ C~~c~~ontractors, Subcontractors or Vendors is obsolete, is not usable, or is not economical or efficient to use, the coalition may surplus or dispose of the property in accordance with OEL s~~S~~urplus or d~~D~~isposal of ~~g~~G~~G~~rant-p~~P~~urchased p~~P~~roperty procedures or the ELC's applicable disposition of property policy and procedure, whichever is applicable. ~~.~~

4. Magnetic media such as hard drives, diskettes, universal serial bus ("USB") flash drives or tapes must be erased and destroyed by ~~Coalition~~ELC's IT ~~Designee~~Department ~~IT/Data Manager~~ before disposal.

5. Uninterruptible power supply ("UPS") is required for networking devices and server(s).

6. Only the ~~Coalition~~ELC's IT ~~Designee~~Department staff ~~IT/Data Manager~~ shall install applications on a server or workstation.

7. Operating systems and system applications must be kept current.

8. ELC's computer network must ~~be secured~~be secured and protected with a network based firewall and antivirus

9. All ELC work (files/documents) must be stored on server.

10. Servers must not be used for general purposes computing such as web browsing or reading emails and must be strictly used for its intended purpose.

11. Equipment checked out to ~~ELC employees~~ELC staff must be utilized for ELC related business. Use of ELC equipment for non-ELC business is prohibited under ELC's policies and procedures. Equipment lost or stolen while in the personal possession of an employee is the responsibility of the employee and must be reported it to their supervisor/IT department immediately. ELC will review any instances of theft or foul play pertaining to the equipment. All ELC ~~employees~~ staff requesting the use of a laptop or any other equipment owned by ELC must complete and sign an **Equipment Checkout Authorization Form** attached hereto as ~~(~~**Exhibit D** and by reference made a part of this policy and procedure. ~~) kept by designee personnel.~~

The ELC complies with the requirements described in OEL"s IT Security Policy~~-~~ regarding~~5.05.02.17,~~ p~~P~~hysical and e~~E~~nvironmental s~~S~~ecurity.

Antivirus

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

In order to protect the ~~and avoid~~ ELC's ~~'s data~~ systems ~~information resources~~ from viruses, malware, spam or other internet attacks, the following steps/actions must be taking by all ~~ELC employees~~ELC staff:

1. Never install software on ELC computers without permission from the ~~Coalition~~ IT Department~~Designee~~~~Data and Network Manager~~.

2. Never download files from unknown or suspicious sources.

3. ~~Employees~~ELC staff ~~cannot~~ should not remove or disable antivirus software from any ELC computers.~~, nor delete spam, chain, and other junk email without forwarding them.~~

4. If a computer virus is suspected, immediately notify your supervisor and/or the ~~Coalition~~ELC's IT ~~Designee~~~~Information~~Department ~~Systems Security Officer~~.

5. ELC staff ~~Information Users~~ are responsible for taking appropriate precautions to avoid introducing viruses or malware into the ELC's computing environment.

6. Antivirus software is set to update automatically as new virus definitions are made available by the vendor.

7. ~~Coalition~~ELC's IT ~~Designee~~Department ~~Data and Technology Director~~ is responsible for deploying antivirus agent to each ELC network computers from the server and to regularly monitor the ELC antivirus console installed on the server to verify that antivirus protects all computer systems:
   a. Antivirus software applies to all servers, workstations, and remote access computers;
   b. ~~.~~Every server or computer that contains OEL data or conducts and~~=y~~ form or OEL business runs antivirus software;
   c. Antivirus software protects data, scan documents, attachments, emails and internet sites before use by staff; Antivirus program scan portable media devices;
   ~~7.~~d. Documentation is maintained to verify the purchase and installation of antivirus software.

Mobile Computing

The use of laptop computers and mobile devices provide flexibility and enhanced communications that allow ELC staff ~~personnel~~ to be more productive. However, the use of these devices outside of the ~~ELC~~

offices of the ELC poses risks to those devices and the information they contain. These devices may also present a hazard to the ELC's data systems ~~information resources~~ upon their return to the ~~ELC~~ office (for example, by spreading a virus that was obtained outside the office). These devices have the capability for direct connectivity to the i~~I~~nternet or other networks outside of the ELC's network which lack the protections afforded by ELC's n~~N~~etwork firewalls and other perimeter protections. Therefore, additional security measures must be implemented to mitigate increased security risks presented by mobile computing. This p~~P~~roceduree~~olicy~~ establishes procedures for mobile computing and applies to all laptops and other mobile computing devices that are used to store or process ELC data.

To protect the ELC's data systems ~~network and other information sources~~ from the security risks mobile devices present when used, the following standards/guidelines must be implemented by ~~ELC employees~~ELC staff:

1. Laptops and other mobile computing devices must be inventoried by ~~the Accounting~~the Accounting and Human Resources Manager and tracked by the ~~designee~~ IT department personnel.

2. Laptops must have antivirus installed with current updated definitions. The firewall must be enabled.

3. ELC confidential data placed on mobile devices must be protected against unauthorized access and encrypted. Storage of ELC confidential data on any mobile device is prohibited.

4. Mobile computer users are responsible for backing up their data that is stored on the mobile computer on a regular basis.

5. ~~ELC employees~~ELC staff are responsible to take reasonable precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.

6. ~~ELC employees~~ELC staff must immediately report their supervisor and/or IT department~~/Data Manager~~~~Data Manager~~ any loss, theft, tampering, unauthorized access, or damage of any mobile device.

7. All ~~ELC employees~~ELC staff requesting the use of mobile devices owned by ELC must complete and sign an **Equipment Checkout Authorization Form** attached hereto as ~~(~~**Exhibit ~~D~~D** and by reference made a part of this policy and procedure~~)~~**.** Any ELC staff ~~employee~~ assigned an ELC mobile device must also complete an **Employee Receipt of Property Form** attached hereto as ~~(~~**Exhibit E** and by reference made a part of this policy and procedure. ~~)~~**.** The Employee Receipt of Property Form ~~(Exhibit E)~~ will be kept by Human Resources Manager for the ELC.~~.~~

~~8.~~ ~~Coalition~~ELC's IT ~~Designee~~Department ~~Information Systems Security Officer (ISSO)~~ is responsible for auditing the use of ELC mobile computing devices to ensure compliance with the procedures and guidelines set forth in this protocol.

~~9.~~8.

~~10.~~9. Equipment checked out to ~~ELC employees~~ELC staff must be utilized for ELC related business. Use of ELC equipment for non-ELC business is prohibited under ELC policies and procedures.

Remote Computing

Remote access to the ELC network provides many benefits. However, remote access to the ELC network ~~via dialup or other connectivity~~ poses a risk of intrusion into the network by unauthorized persons and a risk of interception of the data being transferred through the remote connection. Remote access requires additional security controls to mitigate the increased risks posed by allowing connectivity from outside the ELC office environment. This protocol establishes procedures for r~~R~~emote a~~A~~ccess and applies to all remote connectivity to ELC information resources. This procedure~~olicy~~ is designed to protect ELC information resources and prevent damages to the organizational network or computer systems.

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

~~1.~~ All ~~ELC employees~~ELC staff by default will have account settings set to deny remote access. Only upon request will the account settings be changed to allow remote access. ~~ELC Employees~~ELC staff must read and sign a **Remote VPN Access Form** attached hereto as ~~(~~**Exhibit F** and by reference made a part of this policy and procedure. ~~)~~**.**

~~2.~~1. Only upon of the approval of the **Remote Access VPN Request Form** will the employee be allowed to remote VPN by the ~~Coalition~~ELC's IT ~~Designee~~department.

~~3.~~2. All remote connectivity must be authenticated. Confidential data transferred over a remote access connection must be encrypted to protect it from unauthorized disclosure.

~~4.~~3. All data security policies for use in the ELC office environment must also be observed when using or connecting to ELC resources while outside the ELC office environment.

~~Any equipment including p~~~~Personal home computers used are prohibited from~~to connecting ~~to ELC network. information resources must meet ELC remote access requirements, including having an approved antivirus program installed and configured with the latest updates.~~

~~5.~~4. ELC confidential data is not to be stored on any non-ELC computers. It is the responsibility of ~~the~~ ELC staff~~employee~~ to ensure that their access devices and remote connections are not used by unauthorized persons (including family members).

~~6.~~5. ELC remote ~~Information~~ users may not change operating system configurations, install new software, alter equipment or download software from systems outside of ELC network onto ELC remote access computers.

~~7.~~6. To prevent unauthorized users from accessing confidential ELC information, ELC remote

users must log out up after completing a remote session.

8.7. ELC remote users are responsible for complying with the procedures and guidelines set forth in this protocol; protecting their remote access credentials and devices from disclosure to, or use by, unauthorized persons; and immediately reporting any suspected unauthorized use of their remote access account or any damage to or loss of ELC computer hardware, software, or data that has been entrusted in their care.

9.8. The CoalitionELC's IT DesigneeDepartment IT/Data Data Manager is responsible for auditing the use of remote access to ensure compliance with the procedures and guidelines set forth in this protocol. The CoalitionELC's IT Designee department Data and Network Manager will regularly review remote access audit log.

9. Personal home computers are prohibited from connecting to ELC network.

Games/Purchasing Private Goods and Services

EmployeesELC staff may not use the ELC's data systems computing resources to access, play or use gamesplay games, contests, audio, or video archived materials or any other forms of entertainment; provided, however, that ELC employees may play computer games after hours when ELC offices are not open to the public.

Similarly, employeesELC staff may not use the ELC 's data systems computing resources to purchase personal goods and services over the Internet.

Use of Internet/Worldwide Web

The iInternet/wWorldwide wWeb (collectively the "Internet"), can be a valuable research tool and resource for ELC and its employeesELC staff. However, as with all electronic communications and services, the use of the Iinternet is subject to abuse.

Subject to all policies and prohibitions contained herein, those contained in ELC's Employee Hhandbook, and as otherwise set forth under relevant laws, statutes, regulations and ordinances, employeesELC staff may utilize the Iinternet to conduct ELC business and for limited personal use. However, in utilizing the Internet, ELC employeesELC staff must remain cognizant that:

1. ——Any messages or information sent by an employee to one or more individuals via an electronic network (e.g., bulletin board, on-line service, or Internet) are statements identifiable and potentially attributable to ELC. While some users include personal "disclaimers" in electronic messages, it should be noted that there would still be a connection with ELC, and the statement might still be legally imputed to ELC. All communications sent by employeesELC staff via a network must comply with this and other ELC policies, and may not disclose any confidential or proprietary information.

2. Network services and Iinternet sites can and do monitor access and usage and can identify at least which Early Learning Coalition of Broward County/entity (and often which specific

individual) is accessing their services. Thus, accessing a particular bulletin board or website leaves ELC-identifiable electronic "tracks" even if the employee merely reviews or downloads the material and does not post any message.

3. ~~-~~As previously noted, ELC will allow limited use of electronic mail for personal reasons. Subject to the restrictions noted in this policy, ~~employees~~ELC staff may also access the ~~I~~internet for personal reasons on a limited basis.

4. ~~Employees~~ELC staff may not access personal ~~I~~internet pages through the ELC~~-~~'s data systems~~computing resources~~.

Screensavers

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

Sensitive Information

~~ELC employees~~ELC staff must be cognizant that certain information about providers and individuals affected by our programs is confidential by law or is otherwise sensitive information. Information such as s~~S~~ocial s~~S~~ecurity numbers, financial information or private information concerning children, must be guarded and protected by all ~~employees~~ELC staff.

Accidental Violation of Policy

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

Requirements of Managers and Supervisors

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

Reporting Violations

~~Employees~~ELC staff must report any violations of this policy to Human Resources and in accordance with ELC policies and procedures. ELC may also refer suspected violations of applicable law to appropriate law enforcement agencies.

No Duty to Defend

ELC reserves the right not to defend any employee for any action brought by any person or entity for violation of any law, statute, regulation or ordinance committed by such employee using the ELC's ~~data~~

systemscomputing resources. In addition, ELC reserves the right to seek indemnification or subrogation from any employee in any action to which ELC is made a party based upon the employee's violation of any law, statute, regulation or ordinance.

Questions

If you feel unsure about whether your use of the an ELC 's data systems computing resource violates this policy or any law, statute, regulation or ordinance, or if you have any other questions regarding the use of the ELC's datacomputing systemresources, please ask the CoalitionELC's IT Designeedepartment IT/Data Manager before a problem arises rather than after.

Exhibit A

MEMORANDUM OF UNDERSTANDING

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

I. Designation of System Administrator and Security Officer

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

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

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

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

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

II. Confidentiality and Public Access

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

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

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

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

DATA SECURITY AGREEMENT

I, _____, understand that during my employment or contract, whichever is applicable, with the Early Learning Coalition of Broward County ("ELC"), my employing entity or myself, ~~I~~ will or may be exposed to certain confidential records, data, documents or information pertaining to Office of Early Learning ("OEL") school readiness, voluntary pre-kindergarten, ~~programs~~or other programs and/or resources, which ha~~s~~ves been made available to my employer or ~~loyer, for~~myself, for the limited purpose of performing the~~its~~ public duties on behalf or in partnership with the ELC.~~y pursuant to the Grant Award~~.

This ~~ese~~ confidential information~~records~~ may include but not be limited to, social security numbers, parent and child information, payment, ~~child care~~childcare provider, household demographics, trade secrets, intellectual property, proprietary information, and resource and referral, which are private and confidential and may not be disclosed to others. In order to perform my duties associated with the assessment and reporting requirements set forth in the~~-~~ Florida Statutes and the Florida Administrative Codes as it concerns school readiness and voluntary pre-kindergarten programs~~School Readiness Act~~, I am requesting an approved username, password, and additional instructions on behalf of myself or my employing entity, whichever is applicable~~for~~, for accessing the Enhanced Field System ("EFS"), the Single Point of Entry/~~/~~Unified Wait List ("SPE/UWL") system, and SharePoint (hereinafter referred to as "the Systems"). Prior to receiving such means of access, I, whether on behalf of myself or on behalf of my employing entity, whichever is applicable, ~~-~~acknowledge and agree to abide by the following standards for the receipt and handling of confidential record information.

1. ___I shall not disclose my username, password or other information needed to access the ELC's data s~~S~~ystems to any party, nor shall I give any other individual unauthorized access to this information.

2. ___If I should become aware that any other individual, other than an authorized employee, may have obtained or has obtained unauthorized access to my username, password or other information needed to access the Systems, I shall immediately notify my supervisor, the System Administrator and Security Officer for the early learning coalition. I shall also fill out the required incident report as set forth in the ELC's Incident Report Policy and Procedure.

3. ___I shall not share with anyone any other information regarding access to the s~~S~~ystems unless I am specifically authorized by the ELC ~~early learning coalition~~ or~~-~~ OEL~~the Office of Early Learning~~.

4.____ I shall not access or request access to any social security numbers or other confidential information unless such access is necessary for the performance of my official duties.

5. ___I shall not disclose any individual record data to any parties who are not authorized to receive such data except in the form of reports containing only aggregate statistical information compiled in such a manner that it cannot be used to identify the individual(s) involved.

6. ___I shall retain the confidential data only for that period of time necessary to perform my duties. Thereafter, I shall either arrange for the retention of such information that is consistent with both ~~the~~ federal and~~or~~ s~~S~~tate record retention requirements or delete or destroy such data in accordance with the aforesaid laws.

7. ___I have either been trained in the proper use and handling of confidential data or have received written standards and instructions in the handling of confidential data from the ELC ~~early learning coalition~~ and/or OEL~~the Office of Early Learning.~~. I shall comply with all the confidential safeguards contained in such

training, written standards, or instructions, including but not limited to, the following: a) protecting the confidentiality of my username and password; b) securing computer equipment, disks, and offices in which confidential data may be kept; and c) following procedures for the timely destruction or deletion of confidential data.

8. ___I understand that if I violate any of the confidentiality provisions set forth in the written standards, training, and instructions, my or my employer's, whichever is applicable, user privileges will be immediately suspended or terminated. I further acknowledge that applicable state law may provide that any individual who discloses confidential information in violation of any provision of that section may be subject to a fine and/or period of imprisonment and dismissal from employment. I have been instructed that if I violate the provisions of the law, that I or my employer, whichever is applicable, may receive one or more of these penalties.

9. ___Should I have any questions concerning the handling or disclosure of confidential information, I shall immediately ask my supervisor, or if applicable, a designated representative of the ELC, and be guided by his or her response.

Employee Signature: _____

Date: _____

Early Learning Coalition: _____**ELC Broward**_____

Print Employer Name: _____

Employer Address: _____

_____

Work Telephone: _____

Email: _____

EXHIBIT B

Employment Dates

Start: _____

End: _____

System User Account Form

(Level of Access to Data Systems)

Name of Employee: _____

Employee Title: _____

Immediate Supervisor: _____

Approved to Authorize:
(COFO)

Employee Privilege Levels

Server Access		**Authorization (COFO) Signature**	**Access Completed Date (IT Staff)**	**Access Termination Date (IT Staff)**
Finance				
Executive				
Operations				
• Personnel (access restricted folder)				
• Job Descriptions (access restricted folder)				
• Organizational Charts (access restricted folder)				
• ELC Policy and Procedures (access restricted folder)				
General				
Community				
Program				
Provider Services				
Accountability Monitoring				
Special Projects				
Scan				
ELC Data/System Access				
ELC Website				
EFS				
OEL SharePoint				
ELC SharePoint				
Provider Portal				
Family Portal				
Redetermination Portal				
ASQ				
WELS				

TSG				
Bright Beginnings				
VPK Assessment Orders				
OEL Fraud Referral System				
PICH/TOUCH Reporting				
Refugee Services				
Readiness Rates				
EWS				
MIP				
Dropbox				
Survey Monkey				
Facebook/Twitter/Google+				
Team Shared Email				
vpkimprovement@elcbroward.org				
providerportal@elcbroward.org				
qualityassurance@elcbroward.org				
Agency Access				
Front Door Lock Code				
Building Access Card				
Storage Door Lock Code				

EXHIBIT C

Information Security Training Acknowledgement Form

New Employee: Yes No

Name of ELC Employee: _____

This form acknowledges receipt of the Early Learning Coalition of Broward County's ("ELC's") data~~information~~ security training.

I understand that I may/will have access to confidential information pertaining to the Office of Early Learning programs for the purpose of performing my duties and responsibilities. In order to protect and safeguard the ELC's confidential information, I agree to follow the ELC's Data~~Information~~ Security and Systems Policy~~ies~~ and Procedure~~s within the ELC computing resources policy~~ during my employment with the Coalition.

I have read the above statement and have been provided a copy of the ELC's Data~~Information~~ Security and Systems Policy~~ies~~ and Procedure~~s~~.

My signature acknowledges receipt and understanding of the ELC's data~~information~~ security requirements and training provided by the ~~Coalition~~ ELC IT ~~Designee~~department.

Signature of ELC Employee: _____

Signature Date: _____

EXHIBIT D

Equipment Checkout Authorization Form

Equipment checked out to ~~ELC employees~~ELC staff must be utilized for ELC related business. Use of ELC equipment for non-ELC business is prohibited under ELC policies and procedures. Equipment lost or stolen while in the personal possession of an employee is the responsibility of the employee and must be reported to their supervisor immediately. ELC management will review any instances of theft or foul play pertaining to the equipment. ~~ELC employees~~ELC staff are responsible to take reasonable precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.
Employee Name:
Employee Title:
Employee Signature:
Employee Signature Date

IMPORTANT NOTICE TO ~~EMPLOYEES~~ELC STAFF: Failure to return ELC issued equipment, keys, cell phones, laptops, material, or other items may result in delay of final pay until all ELC property is returned. If these items are damaged or missing, their value may be deducted from the employee's final check.
Property Description:
Tag Number:
Date Removed:
Supervisor's Approval of Removal:
Date Returned:
Supervisor's Acknowledge of Return:

EXHIBIT E

EMPLOYEE RECEIPT OF PROPERTY FORM

Equipment assigned to ~~ELC employees~~ELC staff must be utilized for ELC related business. Use of ELC equipment for non-ELC business is prohibited under ELC policies and procedures. Equipment lost or stolen while in the personal possession of an employee is the responsibility of the employee and must be reported to their supervisor immediately. ELC will review any instances of theft or foul play pertaining to the equipment.

~~ELC employees~~ELC staff are responsible to take reasonable precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.

EMPLOYEE NAME: _____ **DATE RECEIVED: _____**

ITEM DISCRIPTION: _____

SERIAL #:_____ **INVENTORY TAG # _____**

CONDITION RECEIVED: (Circle all that apply) NEW USED BOXED COMPLETE

MISSING PARTS UNWRAPPED DAMAGED

X_____ X_____

Employee Signature **Authorized Signature**

****

DATE RETURNED:_____ CONDITION RETURNED:_____

X_____ X_____

Employee Signature **Authorized Signature**

EXHIBIT F

Remote Access Form

IMPORTANT NOTICE TO ~~ELC EMPLOYEES~~ELC STAFF

Remote access to the ELC network provides many benefits. However, remote access to the ELC network via dial-up or other connectivity poses a risk of intrusion into the network by unauthorized persons and a risk of interception of the data being transferred through the remote connection. It is the responsibility of each ELC employee to ensure that their access devices and remote connections are not accessed or used by unauthorized persons (including family members).

Remote users are responsible for protecting their remote access credentials and devices from disclosure to, or use by, unauthorized persons; and immediately reporting any suspected unauthorized use of their remote access account to the ~~Coalition~~ELC's IT ~~Designee~~ELC~~department~~ ~~Data and Network Manager.~~

Employee Information

Employee Name:
Employee Signature:
Employee Title:
Signature Date