

## Information System Security Policy

### 1.0 PURPOSE:

The intent of this policy is to establish user responsibility and access standards for all information systems, and provide detailed use policies for specific information systems and processes which insures that all appropriate personnel have simple and easy access to timely, accurate and reliable information.

### 2.0 SCOPE:

The scope of this School District policy includes all facilities, owned, managed or leased; all systems; all applications and all users. If you have any questions regarding this policy or the content of this document, please contact your building administrator.

### 3.0 POLICY:

The School District makes every effort to provide its employees with cost effective technologies to support instruction, financial management, office automation and administration. In this regard, the School District has installed or may install at substantial expense and effort, equipment such as computers, computer networks, electronic mail and voice mail systems, etc. It is the responsibility of every employee to ensure the security and integrity of information stored in these systems and compliance with the detailed use policies specified herein. The School District reserves the right to change these policies at any time with or without prior notice, in situations where use of such systems violates or may violate a policy of the organization or violates state or federal law .

### 3.1 ROLES & RESPONSIBILITIES:

All School District Information Systems users and contractors or vendors have specific roles and responsibilities toward the protection of District student, employee or financial information as defined in this policy and in relevant civil and criminal law via regulations promulgated by pertinent external agencies. All staff are accountable for their use of information. System user responsibilities include information protection, information access and reporting violations of this policy. Any additional expectation toward responsibility for security will be addressed as necessary.

#### 3.1.1 DEFINITIONS: Specific Roles and Responsibilities of Information System Users

The typical system user will only have one role, some may have several roles:

3.1.1.1 **Technology Technicians Staff** - Technicians are entrusted with protecting, maintaining, classifying, supporting and administering the information resources of a segment or all of the organization. *Information Systems (IS) personnel* are examples of custodians.

3.1.1.2 **Employee/Staff** - Basic system users who are responsible for protecting the integrity and security of information generated by the School District, regardless of whether in electronic or paper form.

3.1.1.3 **Administration** - Administrators who are responsible for the identification and protection of the School District information assets and effective use of this policy within their operational areas.

3.1.1.4 **Systems Support** - Systems support personnel such as "Computer Technicians," "System Managers," "operators," and "system programmers" authorized to execute system procedures and/or controls affecting access or modification to the School District systems and/or data.

#### 3.1.1.5 **Vendor/Contractor**

Vendors and/or Contractors who are contracted by the organization to perform specific functions during which they may come in contact with information and/or information systems. Contracts with Vendors and/or Contractors will specify that they are required by this policy to maintain their efforts at or above this standard for protection of the School District information.

**3.1.2 Information Protection**

It is the responsibility of all School District employees/system users, personnel, affiliates, and/or vendor/contractors to protect the integrity and security of information generated by the School District, regardless of whether in electronic or paper form. The School District information is to be considered confidential unless otherwise noted as public. The degree of protection implemented to secure information is based on education practice standards, regulation, legislation, sensitivity, confidentiality and whether the nature of content is private or public. These factors will be identified by the respective custodian for all data regarding how data/information is to be protected.

**3.1.3 Responsibility Regarding Violations**

Violation of this policy will put the School District and/or the administrator, teacher or other education support employee at financial or legal risk and result in irreparable damage to students, educators, support staff and the School District. Any breach of confidentiality, misuse of user IDs, numbers, passwords, confidential signatures, codes or information found in and/or obtained from records, information systems of any media type and/or received verbally will constitute a violation of this Policy. Any known or suspected physical or electronic threats to the School District information or its integrity are to be reported immediately through your building administrator. The building administrator is responsible for reporting violations to *the Information Technology Director* in order to execute appropriate corrective course of action and classify the violation. Respective school building/departments are responsible for prompt processing of resulting disciplinary actions based on the classification assessment and any applicable internal or external regulation.

All policy violations are to be reported and classified by severity on the basis of: 1) Exposure Risk and 2) Significance.

- 3.1.3.1 **Group I Violations** - Those violations which produce minimal to moderate exposure, and/or consequences present a matter of minor inconvenience or liability to the School District. Group I Violations will be grounds for immediate disciplinary action, up to but not including termination of information privileges and/or **employment as applicable, and will not result in legal action.**
- 3.1.3.2 **Group II Violations** - Those violations which produce moderate to profound exposure, and/or consequences present a matter of major inconvenience or liability to the School District. Group II Violations will be grounds for immediate disciplinary action, up to and including termination of information privileges and/or employment as applicable, and/or legal action.
- 3.1.3.3 **Group III Violations** - Those violations which are clear breach of law, produce profound exposure, and/or consequences present a matter of major inconvenience or liability to the School District. Group III Violations will be grounds for immediate disciplinary action, up to and including termination of information privileges and/or employment as applicable, and legal action.
- 3.1.3.4 **Repeat Violations** - of Group II or III violations will constitute grounds for immediate termination or legal action.

**3.2 ACCESS STANDARDS**

All areas will be subject to periodic audit by IS personnel, Internal Audit staff, and external auditors for compliance with these policies. Variances are to be reported to the building administrator for correction. To ensure compliance, IS staff will re-audit areas in which security violations are reported.

**3.2.1.1. General Access****3.2.1.1 Access to Facilities**

All areas which contain system equipment must be secured. Facility windows must be secure and doors must lock. Facility construction must include secure entry to areas

which contain system equipment. Access restrictions methods include code, card key, key and/or desk attendant/escort. The level of physical protection is to be identified and based on prudent risk analysis.

**3.2.1.2 Access to Hardware**

- *Portable Hardware* - All portable computing devices are to be used in accordance with strict procedures which regulate maintaining a record of each unit, the type of information that will be stored in the unit, to whom it is assigned, and recovering the units from terminated employees. Each portable computing device must be labeled with a phone number to call for "return instructions" in case the device is lost.
- *Stationary Hardware* - All computer hardware security is provided through, but not limited to: (a) restriction of physical access including securing communication closets (b) network access disconnects and (c) network access control at the operating system level of the main processors, by application. Under no circumstances are personnel not affiliated with the School District to be left unattended while in secured areas.

**3.2.1.3 Access to Documentation**

- *Document Handling* - All information pertaining to the School District, its employees, students and affiliates is considered confidential. Access to confidential information whether in electronic or paper format is to be secured. Only nonconfidential information may be discarded into wastebaskets. School/Building/Department areas which process confidential information will provide document handling procedures including secure storage, retrieval, disposal and destruction processes in order to ensure that confidentiality and security is maintained. Document handling procedures will include School/Building/Department review and self-audit of the process, at minimum, on an annual basis or more frequently as process changes necessitate.
- *Technical Manuals* - *System/Department* documentation manuals will be secured for use by authorized personnel only. A file area will be designated as the master source collection of system/department technical documentation and maintained for each department or area. Any documents physically removed from the source file area must be signed out, by form, so as to identify by whom and when the information was checked out and where it is being kept if retrieval becomes necessary.

**3.2.1.4 The School District Access Rights**

The School District maintains all rights and the ability to enter into any School District system and to inspect and review any and all data recorded in those systems including voice mail and electronic messages left on or transmitted over these systems. Employees should also have no expectation that any stored information will be private, whether the information is maintained on a computer hard drive, computer disks, or in any other manner. Investigations into suspected incidences of impropriety, triggered inadvertently or deliberately, will be conducted as necessary to locate substantive information that is not more readily available by some other less intrusive means. The contents of the School District computers, voice mail, and electronic mail, properly obtained for some legitimate business purpose, may be disclosed if necessary within or outside of the School District subject to restrictions of law and according to other policies dealing with the School District confidential information.

**3.2.1.5 Authorized Access**

Access to information is to be regulated to protect student/employee information and to preserve the business interests of the School District. Only personnel, affiliates, and/or vendor/contractors who have been approved for specific accesses are allowed to use the School District systems. It is the responsibility of such authorized users to protect passwords, access codes, and/or other access keys. Sharing individual passwords and

/or access with anyone, whether a School District employee or not, is a violation of this policy. All unauthorized system access is strictly prohibited.

*Access Criteria* - Regulation of authorized access is to be provided to users through system administration based on the following criteria:

- *Confirmation of User Identity* - Knowledge of user identity is required by a designated trusted source (i.e., system administrator or building administrator) in order to establish access via approved system access request protocol. Access reset requires verification of personal facts maintained on file by IS.
- *Data Classification* - Data elements are categorized in order to classify data for educational or administrative use and protect data by restricting access
- *Level of Authority* - Access levels are to be assigned based on job responsibility and legal authority as defined by the custodian.
- *Need-to-know* - Access is required to provide information for continuation of the School District business processes.
- *Restriction* - Access is restricted by facility, sensitivity or specific information in order to prevent unauthorized disclosure.

#### 3.2.1.6 Network Access

Individual network access security is provided to a user based upon a profile submitted by a designated trusted source that defines information needs and security level authorized to be assigned to a user.

#### 3.2.1.7 Transferring Information to Third Parties

All data tapes and/or system information transferred outside the School District are to be approved in advance by the respective custodian of the data. This process requires the requestor to submit in writing a request for information data transfer which includes the name and address of requestor, media type or other system output requirements, date requested, date or frequency needed, and reason for request. Third party information requests will be reviewed on an ongoing basis and revalidated on an annual basis.

### 3.2.2 User Access

#### 3.2.2.1 Administration and Monitoring

Access to information is administered through the Technology Department, which is responsible, as custodian of the School District information, for ensuring that all student, employee, and business information resources are protected from unauthorized access. Operating system software employed to process data will also control user access to resources and capabilities which are required and have been authorized. All operating system-level based security systems must ensure that users do not access systems or data to which they are not authorized. Application and/or operating system software must also have the capability to identify, journal, report and assign accountability for the functions performed or attempted by a user, and to deny user access to capabilities or resources which have not been authorized. System Administration of log-on security involves the issuing and maintenance of user accounts which defines the amount and type of access for an individual user. The user account is represented by a User ID which is public, and a password which is strictly private. User accounts may be monitored for audit purposes at any time, specific to each user, regardless of information accessed. Responsibility for auditing user accounts is held by the building administrator, custodian, Information Systems, and internal and external auditors. Procedures for providing and monitoring user access are to secure timely and adequate system access for authorized users.

#### 3.2.2.2 User ID and Password

Log-on identification (User ID) codes are issued to individuals for the term of their employment, support staff membership or administrative privileges, or until job status changes warrant changes in file systems access privileges. No generic User IDs and passwords will be issued for use by more than one individual for official administration [application] system environments. Passwords should not be repeated, even if the

application system permits their repetition. User names, passwords and signature codes will not be attached to computers, printers, bulletin boards or in other obvious areas that can be viewed by other employees, students or visitors. Only the authorized user of the User ID is to have access to password and signature code information.

Technology Department analysts will NOT ask a user for a Password.

- *Level of Access* - The level of access per individual or user group is to be determined by department management in conjunction with the custodian of the data. The access levels are to be recorded as security matrices for use during the application process for User IDs.
- *Name Alias/Change* - In the event a user has made a name change, a written request should be made to the appropriate application system manager for a Name Alias/Change to be processed. System application restrictions may require some name fields remain unchanged for tracking purposes.
- *Inactive User ID* - User IDs which remain inactive for ninety (90) days will be disabled. Disabled User IDs may be reenabled by contacting the appropriate system administrator. If the system administrator is unavailable, the Technology Department may be contacted to reenable the User ID. The Technology Department will verify identification of caller by requesting personal information which was previously collected. If identification is not confirmed then the User ID will not be reenabled.
- *Password Reset* - All system passwords are to be reset every one hundred twenty (120) days.

#### 3.2.2.3 **Application for User ID**

- *Existing Access Type Request* - Applications for a User ID are to be completed by the person requesting the User ID according to instructions developed for each application and included as part of the documentation for that application system. User ID requests are to be approved by the building administrator or designee and processed through the system administrator and appropriate systems support personnel. During large system implementations this process can be waived in favor of bulk creation of User IDs by the system administrator or other system support personnel at the direction of the user building administrator or system administrator. As part of the completion of the User ID application form each applicant will be asked to provide three items of personal information not likely to be easily known by others in the workplace. Personal information is used to verify the identity of a person requesting a reset (e.g. after password violations exceed the maximum set for each application system).
- *New Access Type Request* - The system administrator or other system support personnel will process requests for new access types as identified by the custodian pending proper approval by building administrators or their designee and compliance with any systems restrictions. Any changes will result in modified security matrices.

#### 3.2.2.4 **Failed Log-on Attempts**

Applications and operating system security software must record all attempts to logon to each computer system of the School District. If a User ID and password do not match those stored in system security libraries, the system will reject the log-on and inform the user of the rejection. After three (3) User ID and password mismatches, the application system will terminate the log-on process and, when supported, not permit further log-on attempts using that User ID. If a User ID is terminated because of excessive log-on violations, the user must then contact the technology department to have their password reset. If the system administrator is not available, they should then call the Technology Department to have the password reset. The Technology Department analyst will request one or more of the three items of personal information provided during the User ID application process in order to verify the identity of the caller as noted above. If the user is unable to provide the information, the User ID will not be reenabled and the violation will be reported to the user's building administrator for action. Under no circumstance will a password be reset for anyone other than its owner.

**3.2.2.5 Terminal Time-Out**

All operating system level security must force an automatic log-off of terminals and force automatic resetting of passwords after specified intervals of inactivity and preferably, after a number of unsuccessful attempts to access a system.

Established sessions will be terminated if there is no activity on a terminal for 15 minutes (default setting), except in specific, approved circumstances. Administrative PC systems are to utilize screen saver applications which activate after a maximum of 15 minutes inactivity and must be password protected. To request an extension in terminal timeout, the building administrator should be contacted.

**3.2.2.6 Termination/Transfer and User ID**

All terminated employee User IDs must be disabled no later than 24 hours after date of termination. It is the responsibility of each building administrator to notify the Technology Department concerning all User IDs for employees, students or authorized users. The Personnel Department will provide monthly reports of terminating employees.

**3.2.3 PRODUCTION DATA**

The School District, its affiliates and contractors have developed and implemented an integrated base of financial and educational curriculum systems that provide immediate access to accurate and reliable information for administration, management, research, and student instruction. The data offered in these systems are property of the School District and, as such, should be treated as confidential information by all who have access to it, in whatever form it appears. Security of School District, employee, student and business information is both ethically and legally the responsibility of all employees, students and affiliates.

**3.2.3.1 Business Information**

*It is considered unethical and damaging to the School District to release business information to a competitor, vendor or the general public without specific, explicit approval to do so. The Release of this information to contractors or vendors may also be in violation of state and federal laws.*

**3.2.3.2 Employee Information**

The School District employment information and any related process is confidential and is to be accessed according to the personnel department policy for reviewing or accessing employee information. The release of this information may violate State and Federal privacy laws.

**3.2.3.3 Student Information**

All student information data is confidential and is to be handled as outlined in the policy FL Student Records – Family Educational Rights and Privacy Act.

**3.2.3.4 Data Integrity**

Prior to placing an application system from certification into use, it must be verified that required user functions are being performed completely and correctly, and that the specified administrative, technical and physical safeguards are operationally adequate and fully satisfy the applicable regulations and standards relative to the protection of the information.

**3.2.3.5. Data Transmission**

Data is to be transmitted only through a trusted connection (i.e. a secured, dedicated line from point of transmission to receiver). No public transmission is acceptable without proper encryption security and/or in accordance with Third Party Request standards. Section (3.2.1.7)

**3.2.4 CERTIFICATION/TESTING DATA**

Certification / testing data requires protection controls or safeguards by assuring that confidentiality is protected in transmission of data.

**3.2.4.1 Data Integrity**

*Security requirements for data integrity are to be defined by applicable processing procedures, and security specifications approved by the user prior to acquiring or starting development or prior to making substantial changes to existing applications. Design reviews will be conducted at periodic intervals during the developmental process to assure that the proposed design will satisfy the functional and security requirements specified by the data owner.*

**3.2.4.2 Data Transmission**

If for any reason certification or testing data is to be transmitted to a third party, the request must first be approved in accordance with Third Party Request standards. Section (3.2.1.7)

**3.2.5 BUSINESS CONTINUATION**

Each Building Administrator or their designee is responsible for the development and maintenance of contingency plans for functions which include:

3.2.5.1 **Backup** and retention of data and software

3.2.5.2 **Emergency response** actions to be taken to protect property and minimize the impact of the emergency

3.2.5.3 Actions to be accomplished to initiate **recovery** and effect backup or alternate site

3.2.5.4 **Resume normal operations** in the most efficient and cost-effective manner.

3.2.5.5 Minimum acceptable level of **degraded operation** of the essential (critical) systems or functions are to be identified and prioritized to guide backup implementation.

**3.2.6 ENCRYPTION**

Encryption technology may be used as required by the information custodian.

**3.2.6.1 Acceptable Methods**

Encryption technology features

- should include Graphical User Interface (GUI)
- include functions executed using dialog buttons offer full or partial encryption
- execute from either local PC or network drive and
- provide a time and date audit trail of all encrypted files
- provide a method for retrieving lost or forgotten keys
- be compatible with E-Mail
- provide an export feature that encapsulates E-Mail files
- conform to local and/or Federal encryption laws

**3.2.6.2 Approval Process**

Information System Administration must be notified before any encryption process may be used.

**3.2.7 USE OF ELECTRONIC OR COMPUTER-GENERATED SIGNATURE**

Entries in the educational records or other information systems maintained by the School District may be made only by individuals as specified in School Policies and Support Staff Rules and Regulations. All entries in the record and/or other information systems must be dated and authenticated. Authentication may be by written signature, initials or computer key. A facsimile copy is considered an acceptable entry for any portion of the educational record. This policy prohibits a provider or employee from giving his or her code(s) to anyone else to act in a "proxy" capacity.

**3.2.8 PC/LAN**

Personal Computer / Local Area Network (PC/LAN) includes networks and non-terminal [smart] computers within the School District.

**3.2.8.1 Proper Business Use**

Acceptable use of the School District PC/LAN Computer and telephone networks are used only for the purposes for which they were installed; all equipment and software installed on devices are subject to inventory by IS, Internal Audit, or other auditing entities. Equipment inventories will be periodically performed by IS to assure compliance with IS policies and hardware/software standards. It is unacceptable to use equipment which is not in compliance with Information Systems Equipment Standards. Devices or software will be terminated which are not compliant with standards or that have not been approved by Information Systems, particularly if the software or device is using storage, memory, or device ports allocated for district information systems use or if the equipment or software degrades system or network performance or presents a significant security risk to the School District.

**3.2.8.2 Software & Licensing**

Unless the School District, or one of its component organizations, is specifically licensed for a particular software package or the School District holds an unlimited site license to use or install such software, installation use, or copying of software for other employee or personal use is strictly prohibited.

**3.2.8.3 Personal Software**

Only software for which the School District holds a valid and up-to-date license agreement is to be installed and operational on District equipment.

**3.2.8.4 Virus Protection**

Virus protection is expanded to include malware (malicious software), consisting of viruses, trojans, worms, spyware, etc. An enterprise edition anti-virus solution will be required on all computers connected to the school network. The technology department will oversee the automatic updating, scanning and monitoring of the anti-virus system. Users are asked to make wise choices in messaging and browsing practices. Malware can infect a computer via e-mail by just viewing the message, without opening the attachment. Computers can also be infected by clicking on popup windows or visiting infected websites. As always cd's, floppies, USB drives or other means of external storage should always be treated as highly suspect of infection and must be scanned. Users can protect their computers by following a couple of simple practices: 1. View legitimate websites for business and avoid questionable sites. 2. If you are not familiar with the sender of an e-mail it is advisable not to open it.

**3.2.9 PUBLIC NETWORKS/INTERNET****3.2.9.1 Personal Access**

Only World Wide Web (www) helper application installations approved by and properly obtained from the School District are allowed. All public network users (subscribers) are required to have registered web browser applications and assume responsibility for their proper business use.

**3.2.9.2 Proper Business Use**

Proper business use includes the use of or in support of instruction, educational research and technology, and for the purposes of transacting business or using network facilities and services for the School District. The Internet is to be used in a manner that is consistent with accepted School District standards, ethics, security and confidentiality policies. Subscribers are to use the School District computers, networks or systems only for authorized Internet activities. Unacceptable uses include those uses which conflict with the School District, local or national policies and/or standards.

**3.2.9.3 Information Disclosure**

All disclosures are the responsibility of the subscriber. Subscribers should follow the School District, local or national policies and/or standards.

**3.2.9.4 Copyrights**

According to Title 17 of the United States Code, it is illegal to make or distribute copies of copyrighted material without authorization. The only exception is the user's right to make

a single backup copy for archival purposes. From time to time the School District will negotiate contracts with vendors that permit more than one backup copy. In these cases, or unless otherwise defined by the software manufacturer, this policy will be waived. All user/ subscribers have responsibility to respect intellectual property rights of others.

**3.2.9.5 Software Download**

Use of information systems requires user responsibility toward virus protection. All software downloaded from any bulletin board, File Transfer Protocol (FTP), www, and/or service provider is to be treated as infected until scanned.

**3.2.10 VOICE AND ELECTRONIC MAIL**

The School District is committed to privacy. However, on certain occasions, such as if an employee is on leave or has been terminated, authorized School District representatives may retrieve necessary information from local hard drives or network shares. Electronic and telephonic communications and access to same may be assigned, limited and/or monitored by the School District at its discretion.

**3.2.10.1 Personal Access**

Although employees use certain codes to restrict access to computers, voice mail, and electronic mail to protect these systems against external parties or entities obtaining unauthorized access, employees should understand that these systems are intended for business use, and all computer information, voice mail, and electronic mail messages are presumptively considered the School District records.

**3.2.10.2 Proper Business Use**

The School District computers, networks, electronic mail, and voice mail, should be used only for purposes approved by the School District. Always respect the privacy of other users by not sending unwanted electronic mail messages, or misrepresenting yourself when sending E-mail. Any incidental personal information and messages stored on company voice mail and electronic mail systems will be treated no differently from other business-related information and messages.

**3.2.10.3 Privacy**

The School District reserves the right to obtain access to all voice mail and electronic messages left on or transmitted over these systems. Those who use the systems should not assume that such messages are private and confidential or that the School District or its designated representatives will not have a need to access and review this information. To obtain the privilege to have access to the School District electronic mail tools, each student, patron or employee must sign the School District Information Systems Use (EFBC-C) Agreement which acknowledges that there is no expectation of privacy with respect to such systems.

**3.2.11 TELEPHONE/MODEM LINE**

**3.2.11.1 Proper Business Use**

All telephone/modem lines are to be used solely for the purpose for which they were installed. All lines must be registered with Audio/Visual communications for voice or data use and purpose. Any lines not in use are to be disconnected. Any PC/modem combinations are to remain in "ready" status only during the period of time in use.

**3.2.11.2 Facsimiles**

Facsimiles are to be used in accordance with the School District policy. All facsimiles transmitted are to contain the cover sheet, attached to this policy, including the following: Date and Time Sent, Number of Pages Including Cover Sheet, Sender (Name and Phone), Receiver (Name, Facility, Address, and Phone), Responsibility Statement, Contact Name and number to call in the event that the facsimile is misdirected to an incorrect number. Batch facsimile cover sheets may be altered depending upon risk exposure and system tracking capabilities, pending approval from the custodian of the information.

**3.3 COMPLIANCE FORM**

All School District employee and student information, regardless of the form in which it is presented, will not be revealed to parties without the right and need to know for educational purposes or for the successful completion of job duties according but not limited to, this policy and all the School District policies concerning confidentiality and release of information.

This policy shall be made known to all employees, both certified and support personnel at the time of employment or affiliation, as applicable, and each employee shall indicate understanding of this policy through a signed statement at the time of employment or affiliation, kept within the individual's personnel file. Each employee, provider having access to confidential information will, on a periodic basis, but at least once every year, read the policy and again sign a statement of compliance and understanding, which may be accomplished by electronic means, at evaluations or otherwise. This agreement to maintain confidentiality of information is applicable during and after affiliation/employment is terminated.

**3.4 ATTACHMENTS****Attachment 1 EFBC - A**

**Facsimile Transmittal Cover Sheet** - Form to be used for the School District facsimile transmissions. The footer portion of the form is to be changed to reflect the identity of the transmitting department or area. (Use Existing form)

**Attachment 2 EFBC-AB**

**System Security Identification Form** - Form to be completed by each School District system user. The information will be entered into a database and accessed to identify callers who request password reset. Passwords will be issued and reset by IS over the phone only after the caller is able to correctly provide the answer to one or more of three items of personal information.

**Attachment 3 EFBC-C**

**Information Systems Use Agreement** - Agreement completed and signed by all users. The original completed agreement is to be sent to Information Systems Security. A copy of the completed agreement is to be maintained within the personnel file sent to Personnel, if an employee is sent to the building administrator, if a member of the educational staff. The signee may also retain a copy at their discretion.

REFERENCE: (any applicable statutes)

CROSS REFERENCE: CQ: Data Management  
EFBCA: Internet and Other Networks Acceptable Use  
EFEA: Copyrighted Material  
FL: Student, records – Family Educational Rights and Privacy Act (FERPA)