3.0 INFORMATION HANDLING

3.1 Purpose

The purpose of this policy is to ensure that all FCS digital information is properly handled, whether being transmitted within the organization or to a trusted external third party. This document provides guidance on how to handle sensitive district information, including the physical security requirements and the distribution of sensitive information internally and externally.

3.2 Policy

Users are responsible for safeguarding and monitoring FCS information against unauthorized disclosure, modification, and destruction. FCS information must be used only for FCS related business in accordance with its procedures and standards.

Many students, parents, and district employees have entrusted their information to FCS for official purposes, and all employees must do their best to safeguard the privacy and security of this information. Personally Identifiable Information (PII) is **CONFIDENTIAL,** and access must be strictly limited based on operational need for such access. Access will be granted only when a legitimate business need has been demonstrated and access has been approved in advance based on their role and supervisor consent. Access to special hardware and software must be restricted based on business needs.

Employees with access to sensitive information such as PII, FCS internal documents, and documents classified as confidential must not store such data on any removable media, mobile or portable device, unsanctioned cloud storage, or otherwise unencrypted location without approval and should never be stored or shared or transmitted through personal accounts and/or personal devices. This also includes the printing of sensitive information on paper or electronic documents without an approved security process as outlined below.

3.2.1 Safeguards for Documents

All documents containing sensitive information must be stored appropriately to reduce the potential for disclosure. Documents must not be easily accessible to unauthorized individuals and any documents containing sensitive information should be placed with identifying information face down on counters and desks. These documents should not be left out on printers, desks or countertops after business hours and should be placed in locked storage bins, locked desk drawers, or other secure areas. When discarding documents containing sensitive information, use a shredder or place the document in a secure bin specifically designated as a shredding bin where the documents will be retrieved for shredding.

3.2.2 Printers, Copiers, and Fax Machines

Printers, copiers, and fax machines that are used to process sensitive information must be placed in secure locations and areas not easily accessible to unauthorized persons. If equipment cannot be relocated to a secure location, a sign will be posted near the equipment indicating that unauthorized persons are prohibited from viewing documents from the equipment.

All documents containing sensitive information must be promptly removed from the printer, copier or fax machine and placed in an appropriate and secure location. Any documents containing sensitive information that must be disposed of due to an error in printing will be destroyed by shredding or by placing the document in a secure recycling or shredding bin until destroyed.

If a printer, copier, or fax machine jams or malfunctions when printing Confidential or Restricted information, the involved users must not leave the machine until all copies of the sensitive information are removed or are no longer legible. All paper copies of sensitive information must be disposed of by shredding or other methods approved by management.

3.2.3 Faxing Precautions

Sensitive materials should be transmitted through the district secure file transfer system as practicable. Sensitive materials must not be faxed unless an authorized staff member is on-hand at the time of transmission to properly handle the materials at the receiving site, the fax is sent to a locked room to which only authorized employees have access, or a password-protected fax mailbox, after verbal confirmation that the receiving party is on hand to restrict release to an authorized recipient, or recipient is ready. Sensitive information must not be faxed through untrusted intermediaries.

The receipt of sensitive information by fax must be confirmed promptly. All faxes must employ a standard cover page that includes language approved by the district.

3.2.4 Printer Precautions

When printing sensitive information, the user must be present at the printer at the time of printing or use a secure print queue (follow me printing) to prevent the information from being revealed to unauthorized parties or direct the output to a printer inside an area where only authorized employees are permitted to go.

3.2.5 Copy Machine Precautions

Unless permission from the copyright Owner is obtained, making multiple copies of material from magazines, journals, newsletters, and other publications is forbidden unless this is both reasonable and customary business appropriate.

3.2.6 Electronic Safeguards

3.2.6.1 Computer Access

Only employees who need to use computers to accomplish work-related tasks shall have access to computer workstations or terminals. The posting, sharing and any other disclosure of passwords and/or access codes is prohibited. Access to computer-based sensitive information shall be limited to staff members who need the information to perform their work-related duties. Computer displays must be positioned such that the information cannot be readily viewed by unauthorized persons.

3.2.6.2 Sensitive Data Transmission and Storage

All sensitive data must be encrypted while at rest and during transit across public networks to protect it from internal and external threats and provides a second line of defense in high threat areas. The requirements for data encryption are based on its classification, sensitivity, location, and media where it is stored. Sensitive data shall not be stored on any media other than secure services provided by FCS (such as district provided Microsoft OneDrive).

If sensitive information is transmitted over public computer networks such as the Internet, this transmission must take place with encryption facilities. All portable and remote systems storing sensitive information must also employ hard disk encryption systems. In all but a few rare instances, if information is to be protected, then the user must take specific action to enable encryption facilities. Users must be careful about the inclusion of sensitive information in electronic mail messages that are not protected by encryption. See Data Classification for applicable requirements. FCS Technology department will maintain a list of all district provided services that support encryption. Any district provided services that do not support encryption shall not be used for storage of sensitive data.

3.2.6.3 Electronic Mail

Sensitive data, such as confidential documents or PII, shall not be sent via e-mail in an unencrypted format. If an electronic mail message contains sensitive information, users must not forward it to another recipient unless the other recipient is known to be authorized to view the information, or the originator approves the forwarding. Electronic correspondence that contains sensitive data must be clearly labeled as such See Data Classification for applicable requirements.

3.2.6.4 Data Backup

Formal data back-procedures are required for all multi-user systems that support critical business functions. This shall include, but not be limited to, database servers, mainframes, network file shares and other integral systems. At minimum, all backups must follow the following standards:

- Backups must be made of all essential operational data.
- All physical backups must have externally visible labels identifying the classification of the data.
- All backups containing confidential data must be encrypted.
- Backup media must be stored in a secure location.

- Backup media inventories stored offsite must be reviewed on a periodic basis to any detect any inventory losses.
- Backups must be stored in a location approved by Technology Services.

3.2.7 Media Distribution

All media containing sensitive information must be distributed in a secure manner both internally and externally. External distribution of such media from FCS must be logged and authorized by the data owner. If it is necessary to remove computer-readable sensitive information from FCS facilities, this information must be protected with encryption.

3.2.8 Data Auditing

The retention requirements will be driven by applicable legal, regulatory, or business reasons. If such data is found stored beyond the duration of its storage requirements duration, then it will be securely purged.

3.2.9 Destruction of Sensitive Information

3.2.9.1 Written

Documentation that contains sensitive information must be destroyed promptly when it is no longer needed by shredding or placing the information in a secure recycling or shredding bin until the time that it is destroyed.

3.2.9.2 Electronic

Prior to the disposal of any computer equipment, including donation, sale or destruction, the IT Department must determine if sensitive information has been stored on the equipment and delete all sensitive information prior to the disposal of the equipment or obtain a certificate of destruction by a certified 3rd party. See Data Destruction for applicable requirements.

4.0 DATA CLASSIFICATION

4.1 Purpose

The FCS data classification system, as defined in this document, is based on the concept of need to know. This term means that information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive the information. This concept, when combined with the procedures defined in this document, will protect FCS information from unauthorized disclosure, use, modification, and deletion.

4.2 Policy

4.2.1 Classification Labels

4.2.1.1 Data Custodians and Production Information

All information types possessed by FCS must have a designated Owner. Production information is information routinely used to accomplish business objectives. Information Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are instead designated members of the FCS administrative team who act as stewards, and who supervise the ways in which certain types of information are used and protected.

4.2.1.2 Data Custodians and Access Decisions

Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. Owners must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information.

4.2.2 Data Classifications

4.2.2.1 RESTRICTED

This classification label applies to the most sensitive information that is intended for use strictly within FCS. Its unauthorized disclosure could seriously adversely impact FCS, students, employees, and the FCS mission.

Examples could be security audit results, school safety audit results and school safety plans.

4.2.2.2 CONFIDENTIAL

This classification label applies to less-sensitive operational information that is intended for use within FCS. Its unauthorized disclosure could adversely impact FCS, students, employees, and the FCS mission. Information that some people would consider to be private is included in this classification.

Examples include employee performance evaluations, student performance and statistical information, PII, computer passwords, identity token personal identification numbers, and internal audit reports.

Personal Information (PI) is defined in Ga. Code § 10-1-910 et seq. as an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

- Social Security Number;
- Driver license or state identification card number;
- Account number or credit card number or debit card number if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;
- Account passwords or personal identification numbers or other access codes; or
- Any of the above items when not in connection with the individual’s first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised.

PI does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

4.2.2.3 FOR INTERNAL USE ONLY

This classification label applies to all other information that does not clearly fit into the previous two classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact FCS or its employees, suppliers, business partners, or its customers.

Examples include the FCS telephone directory, new employee training materials, and internal policy manuals.

4.2.2.4 PUBLIC

This classification applies to information that has been approved by management for release to the public. There is no such thing as unauthorized disclosure of this information, and it may be disseminated without potential harm.

Examples include product and service brochures, advertisements, job opening announcements, and press releases.

4.2.2.5 Other Labels

Department or division-specific data classification labels are permissible but must be consistent with and supplemental to the data classification system. These supplementary labels might for example include the use of words like “Personnel” or “Financial.”

4.3.3 Labeling

4.3.3.1 Consistent Classification Labeling

Most of the FCS information falls into the **Internal Use Only** category. For this reason, it is not necessary to apply a label to Internal Use Only information. Information without a label is by default classified as **Internal Use Only**.

If information is sensitive, from the time it is created until the time it is destroyed or declassified, it must be labeled with an appropriate data classification designation. Such markings must appear on all manifestations of the information, such as hard copies, removable media and CDs/DVDs. Personnel must not remove or change data classification system labels for sensitive information unless the permission of the Owner has been obtained.

4.3.3.2 Incorrect Labeling

If the recipient of FCS internal information believes that the data classification label accompanying this information is incorrect, the recipient must protect the information in a manner consistent with the more stringent classification labels. Before using this information or distributing it to any other party, such a recipient must check with the Information Owner to ensure that the label currently applied to the information is correct.

4.3.3.3 Information Collections

Personnel who create or update a collection of information are responsible for choosing an appropriate data classification label for the new collection. This label must be consistent with the decisions made by the relevant Owners and generally should be the most restricted classification level found in the collection.

4.3.3.4 Hardcopy

All printed, handwritten, or other paper manifestations of **RESTRICTED** or higher level must have a highly visible sensitivity label on the upper right-hand corner of each page. If bound, all paper manifestations of sensitive information must have an appropriate sensitivity label on the front cover, the title page, and the rear cover. The cover sheet for faxes containing sensitive information must contain the appropriate classification label.

4.3.3.5 Computer Storage Media

All removable media, and other computer storage media containing sensitive information must be externally labeled with the appropriate sensitivity classification. Unless it would adversely affect the operation of an application program, computer files containing sensitive information must also clearly indicate the relevant classification label in the first two data lines.

If information recorded on computer storage media with a higher sensitivity classification is moved to media with a lower sensitivity classification, then the media with the lower sensitivity classification must be upgraded so that its classification reflects the highest sensitivity classification.

4.3.3.6 Additional Public Information Labels

Unless it is unquestionably already public information, all FCS information with a **Public** label must also be labeled “Approved for Public Release” along with the date when the Owner declared the information Public.

4.3.3.6 Voice Recordings

To reduce the chance of unauthorized disclosure, in general, employees must not record sensitive information. If the use of recording devices is an operational necessity, the proper sensitivity classification must be specified at the beginning and end of each segment of sensitive information. In this case, the recording media must also be marked with the most stringent data classification found on the media. In addition, the media must be protected in accordance with the most stringent classification found on the media and erased as soon as practicable. Any recording generated through official FCS duties will receive a classification of no less than **‘FOR INTERNAL USE ONLY’** unless formally approved by appropriate personnel.

4.3.4 Declassification and Downgrading

4.3.4.1 Schedule for Review

To determine whether sensitive information may be declassified or downgraded, at least once annually, Information Owners must review the sensitivity classifications assigned to information for which they are responsible. From the standpoint of sensitivity, information must be declassified or downgraded as soon as practical.

4.3.4.2 No Unauthorized Downgrading

Personnel must not move information classified at a certain sensitivity level to a less sensitive level unless this action is a formal part of the declassification or downgrading process approved by the Owner.

5.0 DATA DESTRUCTION

5.1 Purpose

The storage of sensitive information must be maintained to the shortest period to satisfy legal, regulatory, and business requirements. The purpose of this policy is to establish a standard for the storage and subsequent destruction of stored, sensitive information.

5.2 Policy

All sensitive information must be destroyed or disposed of when no longer needed for business purposes. To support this policy, FCS personnel must review the continued value and usefulness of sensitive information on a periodic basis. The data retention schedule must be reviewed to determine the minimum legal periods that information must be retained. See Data Retention Schedule for applicable requirements.

5.2.1 Destruction and Locked Boxes

All sensitive information no longer being used or no longer needed must be placed in designated locked boxes until such time as authorized FCS personnel or a bonded destruction service picks it up. If no locked disposal boxes are in the immediate vicinity, sensitive information in hardcopy form must be either shredded, while sensitive information in all other forms must be delivered to management for secure destruction. The shredders used for this purpose must create confetti or other similar small particles. Strip-cut shredders must not be used for this purpose. If unable to immediately dispose of information by the recommended method, it may be locked in a secure location.

Erasing or reformatting magnetic media such as removable media is not an acceptable data destruction method. The use of overwriting programs approved by the CTIO is permissible to destroy sensitive information stored on servers or hard drivers. Only after these programs have been used can storage media containing sensitive information be reused, trashed, recycled, or donated to charity.

5.2.2 Destruction Approval

Personnel must not destroy or dispose of potentially important records or information that is not “owned” by them without specific advance management approval. Unauthorized destruction or disposal of FCS records or information will subject the personnel to disciplinary action up to and including termination and prosecution.

Records and information must be retained if they are likely to be needed in the future, regulation or statute requires their retention, or they are likely to be needed for the investigation or prosecution of unauthorized, illegal, or abusive acts. Any questions about data destruction must be referred to the CTIO.

5.2.3 Permissible Destruction

Personnel may destroy FCS records when approval has been granted by documented instructions from the Owner or the Owner’s delegate, or CTIO. The documented instructions must include the type of records that may be destroyed and when, or the records retention and disposition schedule. Destruction is defined as any action that prevents the recovery of information from the storage medium on which it is recorded.

5.2.4 Removable Storage Media

All materials used in the handling of sensitive information, which could be analyzed to deduce the sensitive information, must be destroyed according to methods approved by the CTIO. Examples of removable storage media include, but are not limited to:

- Thumb drives
- External Hard drives
- CD
- DVD
- Backup Tapes

5.2.5 Photocopies

All waste copies of sensitive information that are generated in the course of copying, printing, or other sensitive information handling must be destroyed according to the instructions found in this policy. If a copy machine jams or malfunctions when personnel are making copies of sensitive information, the involved personnel must not leave the machine until all copies of the information are removed from the machine or destroyed beyond recognition.

5.2.6 Equipment Disposal or Servicing

Before computer or communications equipment is sent to a vendor for trade, servicing, or disposal, all sensitive information must be destroyed or concealed according to methods approved by the CTIO. Internal hard drives and other computer storage media may not be donated to charity, disposed of in the trash, or otherwise recycled unless they have been subjected to overwriting processes approved by the CTIO.

6.0 DATA PROTECTION

6.1 Purpose

Encryption supports data privacy and integrity by providing a method to convert electronic information into a format that is readable only by authorized individuals. This policy establishes that encryption for electronic information shall be consistent with FCS need for continued availability of the information. The purpose of this policy is to define the minimal requirements for the use of encryption.

6.2 Policy

All FCS information and systems must meet the data protections listed in this policy to protect the information assets for FCS.

6.2.1 Data-at-Rest

All data that is classified at or above **FOR INTERNAL USE ONLY** must be encrypted at rest in all locations that it resides. The encryption must utilize a non-deprecated standard of encryption cipher. Currently acceptable encryption protocol is Advanced Encryption Standard (AES) 256 bit.

6.2.2 Data-in-Transit

All data that is classified at or above **FOR INTERNAL USE ONLY** must be encrypted in transit on any public network or wireless network. Encryption must utilize a non-deprecated standard of encryption protocol. Currently, the only approved transit protocols are Transport Layer Security (TLS) 1.2 and 1.3.

6.2.3 Data Loss Prevention

Data Loss Prevention (DLP) techniques should be used to prevent and alert Data Custodians to the misuse of all data that is classified at or above **FOR INTERNAL USE ONLY**. Methods of DLP can include:

- Access control restrictions
- Access notifications
- DLP Products
- DLP Capabilities in host solutions

6.2.4 Integrity Checking

Mechanisms will be in place for checking software, firmware, and hardware before they are installed in the environment. Software, firmware, and hardware that is introduced to the network will only be implemented if they are from known sources.