## SECTION VII

## INFORMATION AND TECHNOLOGY SERVICES

### 7.01 INFORMATION AND TECHNOLOGY SERVICES

A. Information and Technology Services is a support service that deals with the preparation, processing, storage, retrieval, and documentation of all information in the school system.

B. Information and Technology Services functions in an advisory and support capacity to the Superintendent of Schools, Clay County School District Staff, Students, and Parents.

C. Information and Technology Services is responsible for the overall control and performance of the following information systems:

   a. Student Information System

   b. Financial Information System

   c. Operational Information System

   d. Personnel Information System

   e. WAN/LAN Support System

   f. E-mail System

D. Services to be provided by Information and Technology Services include:

   a. Programming Support

   b. Computer Hardware Support

   c. Computer Software Support

   d. Instructional Technology Support

   e. Records Management

   f. Automated Data Processing

### 7.02 REPORTS AND FORMS MANAGEMENT CONTROL SYSTEM

A. As a component of the Information System in this district, a reports and forms management control system shall be implemented under the direction of the Director of Information and Technology Services.

B. FUNCTION

This system shall be responsible for the coordination and control of forms currently in use within the school district. It shall also coordinate state and federal reports.

C. AUTHORITY

All district forms used by programs or offices under the jurisdiction of the School Board of Clay County shall be subject to the procedures developed by this system which shall have the authority to review and approve, or deny, the use of all such forms. Decisions made by this system may be appealed to the Director of Information and Technology Services and the Superintendent.

D. DEFINITION

A form shall be defined as any form, memorandum, letter, or method which requests, in two or more work locations, district staff to collect, maintain, and/or report items of information.

E. REPORTS-CONTROL AND FORMS-CONTROL MANAGEMENT SYSTEM COMMITTEE

Pursuant to Chapter 1008, Florida Statutes, a district reports-control and forms-control management system committee shall be established and composed of a majority of classroom teachers appointed by the bargaining agent and school administrators appointed by the School Board. This committee shall be responsible for periodically recommending procedures to the School Board for eliminating, reducing, revising and consolidating paperwork and data collection requirements and submit to the School Board an annual report of ~~it~~ its findings. (Ref. F.S. 1008.385)

## 7.03 PRIVACY

Due caution shall be exercised to protect the privacy of the records of individuals in accordance with State and Federal Standards.

Data is defined as:

a. Employee and Student data

b. Emails within the school district email system or emails used for the communication with staff, students, parents and community stakeholders.

c. Financial data

d. All data contained in on premise servers and cloud instances including but not limited to documentation, pictures, video, and any data that is held inside of a system controlled or purchased by the Clay County District Schools.

B. Data Ownership

a. All data created or generated for use by the School District, is to be used primarily for business purposes and is the District's property.

b. Any data residing on District-owned devices, is considered District's property.

c. School District Data hosted in third-party applications, is still considered the District's property and should be used primarily for business purposes.

d. School District Data hosted on personal devices, is still considered the District's property and should be used primarily for business purposes.

C. The District has the right to access and review all communications, computer files, databases, and any other electronic transmissions contained in or used in conjunction with the District's systems and applications.

D. Staff members should have no expectation that any information on these systems is confidential or private. Review of such information may be done by the District with or without the staff member's knowledge.

E. Collection and retention of information on the political affiliation, voting history, religious affiliation, or biometric information of a student or a parent, is prohibited.

F. Systems and Services are to be used for business purposes. Personal messages via District-owned technology and services should be limited according to the District Network Security Standards and Board policies F.S 119.011. Staff members are encouraged to keep their personal records and personal business at home. In addition, staff members shall be advised that all data and communications are subject to Florida's Sunshine Law.

G. District users are prohibited from sending offensive, discriminatory, or harassing messages.

H. If a staff member's personal information is discovered, the contents of such discovery will not be reviewed by the District, except to the extent necessary to determine whether the

District's interests have been compromised. Any information discovered will be limited to those who have a specific need to know for that information. The administrators and supervisory staff members authorized by the Superintendent have the authority to search and access information electronically.

I. All computers and any information or software on the computers are the property of the District. In addition, staff members may not copy software on any District computer and may not bring software from outside sources for use on District equipment without the prior approval of the Instructional Resources and Information and Technology Services. Such pre-approval will include a review of any copyright infringements, adherence to laws (such as FERPA, HIPAA, and CIPA), virus problems associated with such outside software, system compatibility, and Florida State Standards alignment.

J. See the District Network Security Standards and Board policies concerning staff and student use of e-mail, and staff and student Network and Internet Acceptable Use and Network Responsibility Contract for more details. F.S. 119.011

## 7.04 RECORDS AND ~~E-MAIL~~ EMAIL RETENTION AND DISPOSAL

A. The School Board hereby adopts the records retention schedules published by the Florida Department of State, Division of Library and Information and Technology Services, Bureau of Archives and Records Management as set forth in publications including but not limited to GS1-SL, and GS7 as amended from time to time.

B. The Superintendent, through the ~~Chief Information Officer~~Director of informaion services~~,~~ in collaboration with ~~the Deputy Superintendent and~~ the ~~various~~ Assistant Superintendents, Chiefs, and divisions shall establish a system of guidelines for the retention and destruction of district school records in order to reduce the space required for record storage. Guidelines shall be drafted to include all applicable record retention laws and shall be amended as needed.

C. Records which are designated as permanent in Florida Statutes, and by the Division of Archives, History and Records Management of the Florida Department of State, and those selected by the School Board or Superintendent as having permanent value, may be destroyed only after being photographed or reproduced on film or stored on a Board approved electronic media in accordance with Rule Chapters 1B-24 and 1B-26, Florida Administrative Code. Photographs or micro-photographs, in the form of film or prints made in

compliance with this rule, shall have the same force and effect as the originals and when authenticated, shall be treated as originals for the purpose of admissibility in evidence and record retention.

D. After complying with the provisions of Florida Statutes, the Superintendent is authorized, at his/her discretion to destroy general correspondence over three (3) fiscal years old and other records, papers, and documents over three (3) fiscal years old which are on the retention schedule approved by the Division of Archives, provided such records do not serve as an agreement or understanding or have value as permanent records. However, commodity records are to be maintained five (5) fiscal years. Destruction of other records shall be in accordance with the retention timelines and schedules set forth in the guidelines promulgated by the Superintendent or his/her designee.

E. The School Board recognizes that ~~e-mail~~ email is a media type which has ~~no~~ a ~~specific~~ retention period of seven (7) years at a minimum. ~~The retention period for e-mail documents is determined by the content of the e-mail. The policies for the retention/disposition of e-mail documents are as follows:~~

~~1. PERSONAL MESSAGES - Personal and private e-mail, jokes, spam, chain letters, advertisements and other correspondence which would come under the classification as "junk mail" are not classified as public records. Accordingly, such correspondence shall be deleted immediately upon receipt. E-mail considered personal should be printed out and maintained separate from the e-mail account.~~

~~2. TRANSITORY MESSAGES - E-mail which is intended for the communication of information only, and is not intended to set policy, establish guidelines or procedures, certify transactions, become a receipt or to formalize or perpetuate knowledge is considered "Transitory" in nature. E-mails which meet these parameters shall be deleted as soon as practicable once the individual recipient has obtained the information from the communication and has determined that the e-mail is obsolete, superseded or has lost it administrative value.~~

3. RETAINED MESSAGES - All e-mail not classified as Category 1 or 2 as set forth in the preceding paragraphs shall be retained according to the established retention/destruction guidelines promulgated by the Superintendent or his/her designee in accordance with Department of State Guidelines. Space for storage of such e-mails is of paramount importance. Accordingly, e-mail documents which must be retained should be printed out and stored in paper form in folders specifically created by each individual for such a purpose or stored in electronically created e-mail folders which are clearly labeled "Subject To Public Disclosure ". Because each e-mail category has a specific retention period, e-mails with like retention periods (two years, three years, etc.) shall be stored in the same folder in chronological order thereby facilitating destruction as retention periods expire. In all instances in which e-mail documents or correspondence originated within the district, i.e. employee to employee e-mail, which must be retained pursuant to this sub-paragraph, the record copy shall be retained and maintained by the employee who originated the correspondence. In all instances in which e-mail documents were received from or sent to an e-mail address outside of the district e-mail system, and which must be retained pursuant to this sub-paragraph, the record copy of both the sent e-mail and the received e-mail shall be retained and maintained by the employee who either sent or received said e-mail.

4. CONFIDENTIAL MESSAGES - The use of e-mail for the transmission of confidential information such as confidential student information, identifiable student information, student records and confidential personnel information is discouraged though allowed when carried out in accordance with guidelines adopted by the Instructional Division and Human Resources. In the event that such information is transmitted by e-mail, it must be retained and should be printed out and stored in paper form in a student's records or in the appropriate personnel record or, as an alternative, sequestered in an electronically created e-mail folder that is clearly identified and labeled as either student records or personnel records and labeled "Confidential-Not Subject To Public Disclosure". The individual charged with the responsibility of maintaining the record copy of all such correspondence or documents identified in this sub-paragraph shall be determined in the same manner as is set forth in sub-paragraph "3".

5. ~~PROCESSING REQUIREMENTS - All e-mail shall be processed in accordance with these policies, by the individual holder of the e-mail account, such that all e-mail is either deleted, printed and filed, or segregated into a file folder as set forth herein no later than fifteen (15) days after receipt of an e-mail document or correspondence. Failure to follow these policies shall result in suspension of e-mail privileges.~~

(Ref. F.S. 1001.41, Adopted: 05/15/08) (Revised: XX/XX/XX)

## 7.05 STAFF INTERNET SAFETY POLICY

### A. INTRODUCTION

It is the policy of Clay County District Schools to: (a) prevent staff access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of staff; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)], Fla. Stat. § 1006.1494 (SB 662), Fla. Stat. § 1003.02, Fla. Stat. § 1003.32, Fla. Stat. § 1003.42, Fla. Stat. § 1003.07 (SB 379), Fla. Stat. § 112.22 (SB 258). This policy aims to protect staff and students from inappropriate content, safeguard their personal information, and promote a secure online environment.

### B. DEFINITIONS

Key terms as defined in the Children's Internet Protection Act.

a. **MINOR.** The term "minor" means any individual who has not attained the age of 17 years.
b. **TECHNOLOGY PROTECTION MEASURE.** The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:
c. **OBSCENE.** As that term is defined in section 1460 of title 18, United States Code;
d. **CHILD PORNOGRAPHY,** as that term is defined in section 2256 of title 18, United States Code; or Harmful to minors.

e. **HARMFUL TO MINORS.** The term “harmful to minors” means any picture, image, graphic image file, or other visual depiction that:Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

f. **SEXUAL ACT; SEXUAL CONTACT.** The terms ”sexual act” and ”sexual contact” have the meanings given such terms in section 2246 of title 18, United States Code.

C. ACCESS TO INAPPROPRIATE MATERIAL

To the extent practical, technology protection measures (or “Internet filters”) shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Staff shall take this into consideration, including the subject matter and the age of students that they will be displaying this information to. The information must be age appropriate in accordance with Fla. Stat. § 1003.32.

Specifically, as required by the Children’s Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

D. INAPPROPRIATE NETWORK USAGE

To the extent practical, steps shall be taken to promote the safety and security of Staff and students of the Clay County District Schools online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children’s Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called ‘hacking,’ and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

## E. PREVENTION OF UNAUTHORIZED ACCESS AND UNLAWFUL ACTIVITIES

(a) The district shall enforce technology protection measures to prevent hacking or unauthorized access by saff to data or information they should not have access to.
(b) Staff members shall be prohibited from engaging in any unlawful online activities, including but not limited to hacking, plagiarism, cyberstalking, and distribution of inappropriate or illegal content.

## F. PROTECTION OF STAFF AND STUDENT PERSONAL INFORMATION

The district shall ensure that websites, web or mobile applications, and software used by staff and students adequately protect against the disclosure, use, or dissemination of staff and students' personal information in accordance with FLDOE rule 6A-1.0955, F.A.C.

## G. SOCIAL MEDIA USAGE

Staff shall have access to social media in accordance with the Clay County Employee Handbook (Social Media Guidelines). With the explicit exception of Tik-Tok and any other application as outlined by the Fla. Stat. § 1003.02. Additionally, the use of TikTok, including any successor platforms, is strictly prohibited on all district-owned devices and any device connected to the district- or school-provided internet. TikTok, or any successor platforms, shall not be used to communicate or promote any school district, school, school-sponsored club, extracurricular organization, or athletic team.

## H. SUPERVISION AND MONITORING

It shall be the responsibility of all members of the Clay County School District staff to supervise and monitor age appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act, Fla. Stat. § 1006.1494 (SB 662), Fla. Stat. § 1003.02, Fla. Stat. § 1003.32, Fla. Stat. § 1003.42, Fla. Stat. § 1003.07 (SB 379), Fla. Stat. § 112.22 (SB 258).

All online content for use by students shall require staff to confirm the content is available to students. This can be done through the use of the content filter check for student access. See "Lightspeed student content check procedure" to ensure it is not blocked by CCDS filtering system. If it is found to be blocked, follow the procedure through the school curriculum counsel to get the resources reviewed prior to use.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Information Systems Department.

### I. ANNUAL REVIEW

This internet safety policy shall be reviewed and approved annually by the district school board to ensure its ongoing effectiveness and compliance with state regulations.

### J. REPORTING AND NON-COMPLIANCE

Students, staff, and parents are encouraged to report any concerns related to internet safety or policy violations to designated school authorities. Non-compliance with this policy may result in disciplinary actions as per district guidelines.

## 7.06 STUDENT INTERNET SAFETY POLICY

### A. INTRODUCTION

It is the policy of Clay County District Schools(CCDS) to: (a) prevent student access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)], Fla. Stat. § 1006.1494 (SB 662), Fla. Stat. § 1003.02, Fla. Stat. § 1003.32, Fla. Stat. § 1003.42, Fla. Stat. § 1003.07 (SB 379), Fla. Stat. § 112.22 (SB 258). This policy aims to protect students from inappropriate content, safeguard their personal information, and promote a secure online environment.

### B. SCOPE

The scope of this policy is defined as when a student utilizes the CCDS student account. Additionally, while accessing the CCDS network via wired or wireless with a personal account. This does not include the student using a personal account on a personal device such as a cellular service during non-curriculum time periods.

### C. DEFINITIONS

Key terms as defined in the Children's Internet Protection Act.

a. **MINOR.** The term "minor" means any individual who has not attained the age of 17 years.
b. **TECHNOLOGY PROTECTION MEASURE.** The term " technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:
c. **OBSCENE.** As that term is defined in section 1460 of title 18, United States Code;
d. **CHILD PORNOGRAPHY,** as that term is defined in section 2256 of title 18, United States Code; or Harmful to minors.
e. **HARMFUL TO MINORS.** The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
f. **SEXUAL ACT; SEXUAL CONTACT.** The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.

## D. ACCESS TO INAPPROPRIATE MATERIAL

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information, taking into consideration the subject matter and the age of students at each school.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

## E. INAPPROPRIATE NETWORK USAGE

To the extent practical, steps shall be taken to promote the safety and security of students of the Clay County District Schools online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

## F. PREVENTION OF UNAUTHORIZED ACCESS AND UNLAWFUL ACTIVITIES

(a) The district shall enforce technology protection measures to prevent hacking or unauthorized access by students to data or information they should not have access to.
(b) Students shall be prohibited from engaging in any unlawful online activities, including but not limited to hacking, plagiarism, cyberstalking, and distribution of inappropriate or illegal content.

## G. PROTECTION OF STUDENTS' PERSONAL INFORMATION

The district shall ensure that websites, web or mobile applications, and software used by students adequately protect against the disclosure, use, or dissemination of students' personal information in accordance with rule 6A-1.0955, F.A.C.

## H. SOCIAL MEDIA USAGE

Students shall be prohibited from accessing social media platforms while utilizing the district resources or the district provided account.

## I. SUPERVISION AND MONITORING

It shall be the responsibility of all members of the Clay County School District staff to supervise and monitor age appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act, Fla. Stat. § 1006.1494 (SB 662), Fla. Stat. § 1003.02, Fla. Stat. § 1003.32, Fla. Stat. § 1003.42, Fla. Stat. § 1003.07 (SB 379), Fla. Stat. § 112.22 (SB 258).

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Information and Technology Services Department.

J. ANNUAL REVIEW

This Internet Safety Policy shall be reviewed and approved annually by the district school board to ensure its ongoing effectiveness and compliance with state regulations no later than September 1st.

K. REPORTING AND NON-COMPLIANCE

Students, staff, and parents are encouraged to report any concerns related to internet safety or policy violations to designated school authorities. Non-compliance with this policy may result in disciplinary actions as per district guidelines.

## 7.07 ELECTRONIC DATA SECURITY BREACH NOTICE REQUIREMENTS

A. DISCLOSURE

a. The School Board shall follow all federal and state guidelines regarding data security and privacy and will take reasonable measures to protect and secure data containing personal information in electronic form and shall provide notice of a security breach pursuant to law.

B. All departments will report to Information and Technology Services any suspected breach for investigation and follow-up. Information and Technology Services will notify and inform the Superintendent or designee within 4 hours preliminary information on the breach and escalation recommendations.

C. NOTICE OF SECURITY BREACH

a. Individuals

i. The Superintendent is to provide notice to each individual whose personal information was, or the Superintendent reasonably believes to have been, accessed as a result of a breach.

ii. Notice shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the Superintendent to determine the scope of the breach, to identify the individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than

thirty (30) days after the determination of a breach or reason to believe a breach occurred.

1. If a Federal, State, or local law enforcement agency, determines that notice to individuals would interfere with a criminal investigation, the notice shall be delayed upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary.

2. The law enforcement agency may, by a subsequent written request, revoke the delay as of a specified date or extend the period set forth in the original request.

iii. Notice to the affected individuals is not required, if, after an appropriate investigation and consultation with relevant law enforcement agencies, the Superintendent reasonably determines that the breach has not and will not likely result in identity theft or other financial harm to the individuals whose personal information has been accessed.

1. Such a determination must be documented in writing and maintained for at least five (5) years.

iv. The notice to an affected individual shall be made by written notice to the affected individuals mailing address, or by email sent to the e-mail address of the affected individual.

v. The notice shall include, at a minimum:

1. the date, estimated date, or estimated date range of the breach;

2. a description of the personal information that was accessed or reasonably believed to have been accessed;

3. a contact person and method that the individual can use to inquire about the breach and the personal information maintained about the individual;

4. information about the rights of parents or guardians of students who are under sixteen (16) years of age, incapacitated, or disabled, to request that the student's credit be frozen pursuant to F.S. 501.0051.

vi. The Superintendent may provide substitute notice in lieu of direct notice if such direct notice is not feasible because:

1. the cost of providing notice would exceed $250,000
2. the number of affected individuals exceeds 500,000 persons
3. The School Board does not have an email or mailing address for the affected individuals.

vii. The substitute notice must include a conspicuous notice on the Board website, notice in print, and broadcast media including major media in urban and rural areas where the affected individuals reside. (F.S. 501.171)

viii. Upon receiving notice of a breach of security of a system maintained by a third-party agent, the Superintendent shall notify all affected individuals according to the procedures in this section.

b. State and Credit Agencies

i. In addition to providing notice to the affected individuals according to the procedures above:

1. For any breach of security affecting 500 or more individuals in the State, the Superintendent must provide written notice of the breach to the Florida Department of Legal Affairs in accordance with the requirements in F.S. 501.171.
2. For any breach of security affecting 1,000 or more individuals at a single time, the Superintendent must notify, without reasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. 1681a(p), of the timing, distribution and content of the notices.

c. Security Freeze on Student Credit Pursuant to F.S. 501.0051, parents or guardians of students who are under sixteen (16), incapacitated, or disabled, may have a security freeze placed on the student's credit in the event of a breach of security of personal information.

i. The parent or guardian must submit a request to the consumer reporting agency with proof of authority and identification and pay a fee not to exceed $10 to secure and/or remove the freeze.

1. However, no fee is required if the parent or guardian has documentation showing that the individual has been the victim of identity theft.

2. Upon request of a parent or guardian of a student under sixteen (16) years of age, incapacitated or disabled, who has been the victim of identity theft, the Superintendent shall provide documentation that is within the care, custody, or control of the Board sufficient to invoke the fee waiver under the law.

3. This documentation may be a copy of a valid investigative report, an incident report, or a complaint with a law enforcement agency about the unlawful use of the protected consumer's identifying information by another person.

ii. In addition, the Superintendent shall annually provide parents and guardians of students younger than sixteen (16) years of age, disabled, or incapacitated information regarding their rights under this law.

D. ENFORCEMENT

a. Violations of this policy could result in substantial civil penalties and subject employees to disciplinary action for failure to comply.

b. The provision of notice and information pursuant to this policy is not an admission that the information breach was caused by the Board either directly or indirectly.

c. This policy does not create a private cause of action against violators.

F.S. 501.171, 501.0051

## 7.08 INCIDENT RESPONSE AND DISASTER PREPAREDNESS

A. Incidents are defined as an abnormal, unexpected or caused failure of a system, data corruption, or data access by unauthorized individuals. In order to properly prepare against incidents Information and Technology Services will create and

maintain an Incident Response Plan (IRP). This plan will document the common types of incidents such as but not limited to: Phishing emails, Account compromise, data leaks, malware and virus attacks.

a. The IRP will be tested and validated semi-annually in June and December.

B. Information and Technology Services will prepare and plan for disasters by utilizing a Risk Assessment Plan (RAP) which is part of the Disaster Resource Plan (DRP) which will catalog various risks that may be expected and identify actions to be taken in the case of a disaster event. Events such as but not limited to: hurricanes, floods, train accidents, server failures, and incidents should be assessed and ranked to properly plan budgeting and resources.

a. The DRP will be tested and validated semi-annually in June and December.

C. Legal or criminal activities documented or conducted on district owned devices will be turned over to the Clay County School District Police Department (CCDSPD). District staff will notify the appropriate personnel that an activity was identified as well as the individuals associated with the activity but all data will be protected and documented for the CCDSPD. District staff are not compelled to notify employees or students that the activity was identified and CCDSPD was notified.

D. Data backups of all critical services are conducted IAW the specified Information and Technology Services Data backup procedures.

F.S. 1001.41, 1001.52, 1002.22, 1003.25
F.A.C. 6A-1.0955, 6A-1.9555
20 U.S.C. Section 1232f through 1232i (FERPA)
20 U.S.C. 7908
26 U.S.C. 152
20 U.S.C. 1400 et seq., Individuals with Disabilities Act
Privacy Rights of Parents and Students - P.L. 90-247

## 7.09 CLAY STANDARD TECHNOLOGY

A. Clay Standard

a. The devices and installations Information and Technology Services currently supports are notated by “Clay Technology Standard Quotes” link on the Classlink

Portal available to all administration and Information and Technology Services employees.

i. As new standards are created, this page will be kept up to date with the current technology models that meet or exceed the School District's requirements.

ii. Administrators may purchase off of these quotes freely.

B. Device Classification

a. District Devices

i. District Devices are classified as any device provided by Information and Technology Services and/or enrolled into a management platform sponsored and maintained by Information and Technology Services.

ii. District devices are provided network access by Information and Technology Services Employees or through a provisioned network with access to appropriate resources.

iii. These devices will have varying levels of support based on the available technologies and systems of the School District.

b. Personal Devices

i. Personal Devices are classified as devices not provided by Information and Technology Services or enrolled into a management platform.

ii. Personal devices connected to the OneClay network are not authorized.

1. Personal devices present an unknown risk and danger to the network and data contained within.

iii. Any personal devices should be limited to the "guest" network provided by Information and Technology Services.

1. These devices will not be plugged into the network and are only permitted on the Guest WiFi network.

c. Vendor Devices

i. Vendor Devices are classified as devices or tools needed to perform functions that the School District paid for used by an individual or company.

ii. Vendor(s)/Contractor(s) must have a Network Usage Agreement form on file with Information and Technology Services with indications of what systems that the personnel need access to.

iii. Information and Technology Services will provide network access based on minimum rights to perform specific functions.

d. Donated Devices

i. Any devices received through a donation or crowdfunding source must be provided to Information and Technology Services for a health check and enrolling into a management system.

ii. Devices that do not pass these checks must be returned or surveyed immediately.

C. Official messages and transactions should be conducted via official channels and technologies. Texts, chats, and communications are to be conducted on district owned devices or services in order to comply with federal and state regulations and policies.

(Ref. F.S. 1001.41, Adopted: XX/XXXX)