Liberty County School District

Technology Disaster Recovery Plan (TDRP)

The School Board of Liberty County, Florida

Information Technology Statement of Intent

This document delineates our procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our students, staff, systems, and data.

Our mission is to ensure information system uptime, data integrity, data availability, and business continuity.

- The District shall develop a comprehensive Technology Disaster Recovery Plan (TDRP).
- A risk assessment shall be undertaken to determine the requirements for the TDRP.
- The TDRP should cover all essential and critical infrastructures elements, systems and networks, in accordance with key business activities.
- The TDRP should be tested annually to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the TDRP and their own respective roles.
- The TDRP is to be kept up to date to take into account changing circumstances.

Objectives

The principal objective of the TDRP is to develop, test and document a well-structured and easily understood plan which will help the District recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and/or business operations.

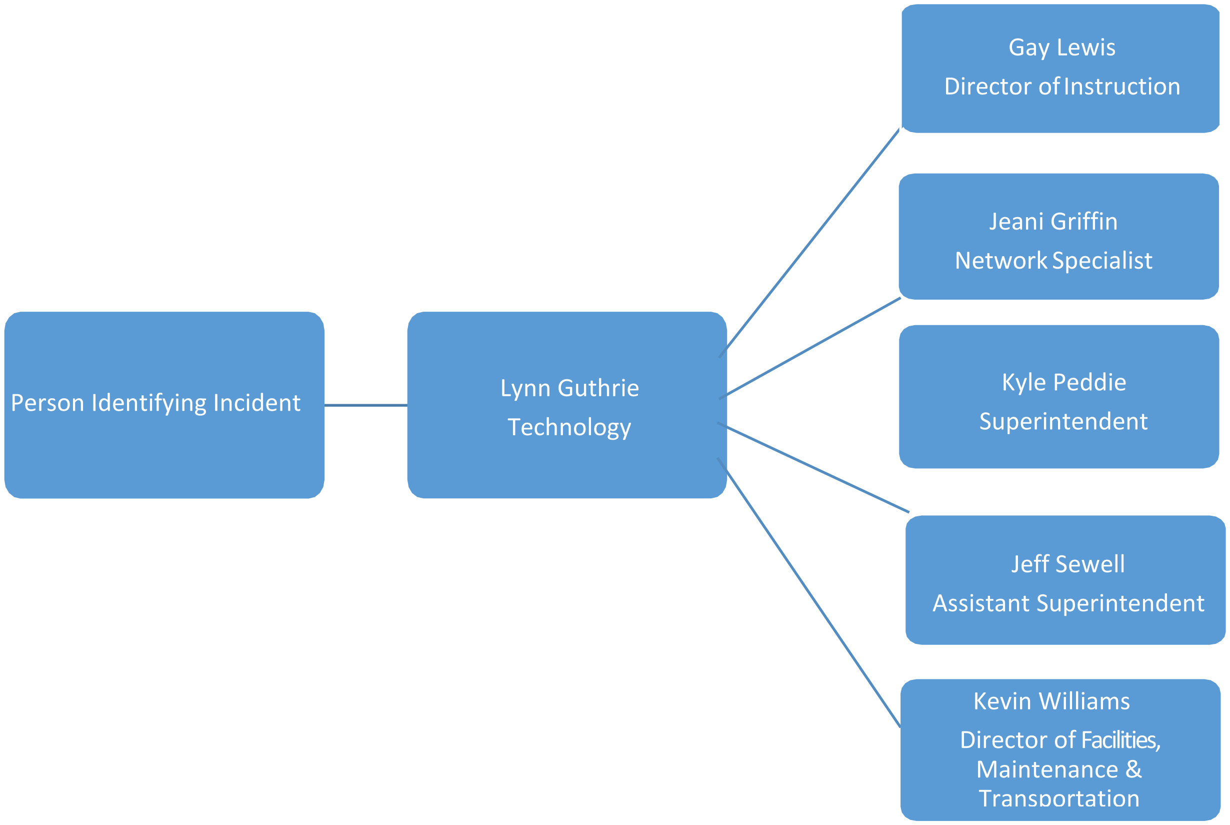
Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective

Key Personnel Contact Information

Name	Phone Number	Email Address
Jeff Sewell Assistant Superintendent	850.643.2275 X 11236	jeff.sewell@lcsb.org
Kevin Williams Director of Facilities, Maintenance & Transportation	850.643.6071	kevin.williams@lcsb.org
Lynn Guthrie Technology Coordinator	850.643.2275 X 11248	lynn.guthrie@lcsb.org
Gay Lewis Director of Instruction (Technology Supervisor)	850.643.2275 X 11233	gay.lewis@lcsb.org
Jeani Griffin Network Specialist	850.643.2275 X 11351	jeani.griffin@lcsb.org
Kyle Peddie Superintendent	850.643.2275	kyle.peddie@lcsb.org

Notification Calling Tree



External Contacts

Panhandle Area Educational Consortium – Finance & HR	Phone Number	850.638.6131
Panhandle Area Educational Consortium – Student	Phone Number	850.892.2187
SchoolinSites – Web Hosting	Phone Number	800.605.1033
	Email Address	support@schoolinsites.com
Uniti/ITS - Voice	Phone Number	866.512.8324 (ITS NOC)
	Phone Number	334.567.1993
	Email Address	Barry.franklin@uniti.com
Uniti/ITS - WAN and Internet Access	Phone Number	334.567.1993
	Email Address	Barry.franklin@uniti.com
Cloud59 Networks - Matt Boyette	Phone Number	478.278.6453
Accelutech – Mark Johnson	Phone Number	478.414.8424

1 Plan Overview

1.1 Plan Updating

The TDRP updating process needs to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the direction of the Technology Coordinator.

1.2 Plan Documentation Storage

Copies of this plan will be stored in secure locations to be defined by Liberty County School District and shared with stakeholders within the LCSB.org domain. Key Personnel will be issued a hard copy of this plan to be filed at home.

1.3 Backup Strategy

Business processes and the agreed backup strategy for each are listed below. If the chosen strategy is for a fully copied, off- site backup, this data will be stored in an off-site facility away. If the chosen strategy is for a fully copied, on-site backup, this data will be stored in a separate location than the current production copy.

VENDOR	BACKUP
FOCUS – SIS	Fully copied, Off-Site Backup
PAEC – HR & Property	Fully copied, Off-Site Backup
Mosaic – Lunchroom System	Fully copied, Off-Site Backup
Destiny – Library System Data	Fully copied, On-Site Backup
Skyward – Finance	Fully copied, Off-Site Backup
Domain Controller, Shared Drives	Fully copied, Off-Site Backup
PowerSchool Eval System	Fully copied, Off-Site Backup

1.4 Risk Management

There are potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

Potential disasters have been assessed as follows:

Potential	Probability Rating	Impact Rating	Description of Potential Consequences & Remedial Actions
Flood	5	3	All critical equipment is located on 1st floor.
Fire	5	3	
Tornado	5	3	
Electrical storms	3	3	Use of surge protectors on all servers to protect from damage.
Hurricane	5	3	
Act of sabotage	4	3	
Electrical power failure	2	4	UPS devices are used to help with quick power outages.
Loss of communications	3	3	

Probability: 1 – Very High, 5 – Very Low; Impact: 1 – Total Destruction, 5 – Minor Annoyance

2.0 Emergency Response

2.1 Alert, escalation and plan invocation

2.1.1 Plan Triggering Events

Key trigger issues that could lead to activation of the TDRP are:

- Total loss of all communications for more the 6 hours
- Total loss of power for more than 6 hours
- Flooding of the premises
- Loss of the building
- Fire effecting network equipment or communications

2.1.2 Assembly Points

Where the premises need to be evacuated, the TDRP identifies two evacuation assembly points:

- Primary - Main parking lot of school or facility;
- Alternate - Liberty County High Athletic Complex

2.1.3 Activation of Emergency Response Team

- When an incident occurs the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the TDRP must be invoked. Responsibilities of the ERT are to:
- Respond immediately to a potential disaster;
- Assess the extent of the disaster and its impact on the business, data center, etc.;

- Decide which elements of the TDRP should be activated;
- Establish and manage disaster recovery team to maintain vital services and return to normal operation;
- Ensure employees are notified and allocate responsibilities and activities as required.

2.2 Disaster Recovery Team

The team's responsibilities include:

- Establish facilities for an emergency level of service within 8.0 business hours;
- Restore key services within 8.0 business hours of the incident;
- Recover to business as usual within 8.0 to 48.0 hours after the incident;
- Report to the Administration

2.3 Emergency Alert, Escalation and Disaster Recovery Plan Activation

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The TDRP will rely on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the District returns to normal operating mode.

2.3.1 Emergency Alert

The person discovering the incident calls a member of the Emergency Response Team in the order listed:

- Emergency Response Team
- Principal/Assistant Principals
- District Administration
- Facilities
- Technology Coordinator
- Director of Maintenance & Transportation

The Emergency Response Team (ERT) is responsible for activating the Disaster Recovery Plan for disasters identified in this plan, as well as in the event of any other occurrence that affects the District's capability to perform normally.

One of the tasks during the early stages of the emergency is to notify the Disaster Recovery Team (DRT) that an emergency has occurred. The notification will request DRT members to assemble at the site of the problem and will involve sufficient information to have this request effectively communicated.

2.4 Coordination with First Responders

- Coordination with local law enforcement and EMS Centers as needed
- Sustaining awareness of restricted movement and curfew conditions (ensuring staff are traveling when allowable).
- Reporting of service restoration progress to Federal, State and Local authorities as needed

3 Media

3.1 Media Contact

Assigned staff will coordinate with the media, working according to guidelines that have been previously approved and issued for dealing with post-disaster communications.

3.2 Media Strategies

Have answers to the following basic questions:

- What happened?
- How did it happen?
- What are you going to do about it?

3.3 Media Team

The Superintendent of Schools or Designee will be the sole communicator for all media.

4 Financial and Legal Issues

4.1 Financial Assessment

The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the District and report their findings to the Director of Finance. The assessment should include:

- Loss of hardware costs
- Labor cost
- Consultant costs

5 TDRP Exercising

TDRP exercises are an essential part of the plan development process. In a TDRP exercise no one passes or fails; everyone who participates learns from exercises -what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Successful TDRP launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens.

Appendix A - Technology Disaster Recovery Plan Templates Disaster Recovery Plan for FOCUS

Student System

SYSTEM	FOCUS Student System
OVERVIEW	
PRODUCTION SERVER	Location: Hosted off-site by FOCUS School Software LLC DNS Entry: Liberty.focusschoolsoftware.com
KEY CONTACTS	PAEC – Student SIS
BACKUP STRATEGY FOR SYSTEM Scenario 1: Total Loss of Data Scenario 2: Total Loss of Hardware	Contact PAEC and they will begin the restore of data. Server is a virtual machine. PAEC will create a new machine on a new server and move application over.
CONTACTS	PAEC Student – Aaron Nicely 850.257.7426 Jenna Chason 850.544.4728

Finance System

SYSTEM	Skyward Finance & Property
OVERVIEW	
PRODUCTION SERVER	Location: Hosted off-site by Skyward ISC Corp DNS Entry: https://skyward.iscorp.com/scripts/wsisa.dll/WService=wsfinlibertycoflpaec/seplog01.w
KEY CONTACTS	PAEC – Finance & HR
BACKUP STRATEGY FOR SYSTEM Scenario 1: Total Loss of Data Scenario 2: Total Loss of Hardware	Contact PAEC and they will begin the restore of data. Server is a virtual machine. PAEC will create a new machine on a new server and move application over.
CONTACTS	PAEC – James Goines 877.873.7237 Sheila Hall 850.447.1867

TDRP for Heartland Mosaic Lunch System

SYSTEM	Heartland Mosaic
OVERVIEW	
PRODUCTION SERVER	Location: Hosted off-site by Heartland DNS Entry:
KEY CONTACT	Joyce Fountain
DISASTER RECOVERY PROCEDURE	
Scenario 1: Total Loss of Data	N/A
Scenario 2: Total Loss of Hardware	Once faulty hardware is isolated, District will replace equipment or contact vendor if under warranty.
CONTACTS	Heartland – Joyce Fountain 800.724.9853 Stacie Fant 850.643.6227

TDRP for Local Area Network (LAN)

SYSTEM	District Local Area Network
OVERVIEW	
PRODUCTION SERVER	Location: District Wide
KEY CONTACT	Jeani Griffin
BACKUP STRATEGY FOR SYSTEM	
Weekly	Backed up nightly off-site
Monthly	As Needed
Quarterly	As Needed
DISASTER RECOVERY PROCEDURE	
Scenario 1: Total Loss of Data	District will contact Network Consultant.
Scenario 2: Total Loss of Hardware	Once faulty hardware is isolated, District will contact Network Consultant for recommendation if needed.
CONTACTS	Jeani Griffin – 850.447.4381
Data	Matt Boyette – 478.278.6453
Hardware	Accelutech/Mark Johnson – 478.414.8424

TDRP for Wide Area Network (WAN)

SYSTEM	District Wide Area Network
OVERVIEW	
PRODUCTION SERVER	Location: District Wide
KEY CONTACT	Jeani Griffin
BACKUP STRATEGY FOR SYSTEM	
Daily	N/A
Monthly	N/A
Quarterly	N/A
DISASTER RECOVERY PROCEDURE	
Scenario 1: Total Loss of Data	Isolate issue to determine if problem is ITS or District. If it's a District owned appliance that is faulty start Disaster Recovery Plan for LAN. If non-district, contact ITS. Once faulty hardware is isolated, District will contact Network Consultant for recommendation
Scenario 2: Total Loss of Hardware	Once faulty hardware is isolated, District will contact Network Consultant for recommendation if needed.
CONTACTS	Jeani Griffin – 850.447.4381
	Uniti/Barry Franklin – 334.850.0364
Hardware	Uniti/ITS NOC – 866.512.8324
	Accelutech/Mark Johnson – 478.414.8424
	Cloud 59/Matt Boyette – 478.278.6453

TDRP for Voice Communications

SYSTEM	Voice Communications
OVERVIEW	
EQUIPMENT	Uniti/ITS
KEY CONTACT	Lynn Guthrie
BACKUP STRATEGY FOR SYSTEM	
Daily	
Monthly	
Quarterly	
DISASTER RECOVERY PROCEDURE Scenario 1: Total Loss of Voice Scenario 2: Total Loss of Hardware	Contact Uniti/ITS NOC Once faulty hardware is isolated, District will contact vendor for recommendation.
CONTACTS	Lynn Guthrie – 850.643.8825 Jeani Griffin – 850.447.4381 Uniti/Barry Franklin – 334.850.0364 Uniti/ITS NOC – 866.512.8324 Cloud 59/Matt Boyette – 478.278.6453

Information Technology Department
Outline and Procedures

1.0 Overview

The IT Department's intention for publishing Policies and Procedures is to provide clear guidelines and expectations aligned with established mission of providing users with the best resources possible to educate every student. The IT Department is committed to protecting Liberty County School District's users from illegal or damaging actions by individuals, either knowingly or unknowingly. Network related systems, including but not limited to computer equipment, software, operating systems, storage media, mobile devices, network accounts providing electronic mail and or resources, WWW browsing, and FTP, are the property of Liberty County School District. These systems are to be used for educational and school business-related purposes with the intent of serving the interests of the students, teachers, and other staff members of Liberty County School District. Maintaining a network requires proper planning, organization, monitoring, and effective security. A team effort involving the participation and support of every liberty County School District employee and affiliate is required to meet and exceed the standards set forth by Florida State Law, Federal Law, the Liberty County School Board and administrators. It is the responsibility of every computer user to know these guidelines, and to govern themselves accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of the network-related systems within the Liberty County School District. These rules are in place to protect the students, staff, and the Liberty County School District. Inappropriate use, improper planning, and disregard of these procedures exposes Liberty County School District to risks including compromise of network systems and services, possible damage to the network, and legal issues.

3.0 Scope

This policy applies to students, employees, contractors, consultants, temporary employees, authorized guests, and other workers at Liberty County School District, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Liberty County School District to include all future purchases.

4.0 Acceptable Use Policy

4.1 General Use and Ownership

- Users should be aware that the data they create on the network remains the property of the Liberty County School District. Users should have no expectations of expressed or implied privacy.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Network/Internet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- Using the Liberty County School District network is a privilege. As with all privileges, it is the responsibility of the user to use this service appropriately and in compliance with all school board policies and procedures, Florida state law, and Federal laws.
- The use of excessive bandwidth and reproduction of copyrighted materials is strictly forbidden and will result in the termination of network services.
- The Liberty County School District assumes no responsibility for costs associated with loss or damage to devices not owned by Liberty County School District while on the network.
- For security and network maintenance purposes, the IT Department may monitor equipment, systems, and network traffic at any time.
- The Liberty County School District's IT Department reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security

4.2.1 Passwords, Accounts, and Antivirus

- Users, which includes employees and students of Liberty County School District, will be granted access to the network after they have signed the Acceptable Use Policy form and forwarded them to designated administrator.
- Users must keep passwords secure and should not share their accounts. Authorized users are responsible for the security of their passwords and accounts.
- Users shall not leave computer unattended while logged on.
- Users of Windows based computer's will be required to change their passwords every 60 days as prompted automatically by Windows Active Directory.
- Users needing password resets for various programs must contact the IT Department. Every attempt will be made to identify the user by positive identification. This method may include sight/voice reconciliation, a predetermined security question, or other questions as determined by the Technology Coordinator.
- All computers used by students, employees, or guests that are connected to the Liberty County School's network, whether owned by the user or Liberty County School District, shall be continually executing virus-scanning software with a current virus database.
- Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, ransomware or Trojan horse code.

4.2.2 Network Security and Administrator Rights

- Administrative passwords for the network, servers, computers, wireless access points, and other electronic devices are to be kept strictly confidential and known only by the IT staff members that need them to perform their duties. Distributing passwords of any kind is strictly forbidden.
- Wireless access points will be secured with a security mechanism to be determined by the IT Administrator. Any attempt to circumvent and/or distribute ways to circumvent this security mechanism is strictly forbidden.

4.3 Sensitive and Confidential Information

4.3.1 Definition and Protection

When handling sensitive and confidential information, precautions must be taken to prevent unauthorized access to the information. Staff members may not disclose sensitive information to persons not authorized to receive it. This includes non-public information such as Social Security Numbers, credit card numbers, bank account numbers, health information, or other confidential student and user data.

Access to student data is limited by Statute. Section 1002.22(3)(d) F.S. guarantees every student a right of privacy with respect to his or her educational needs. In addition, the Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. 123g; 34 CRF Part 99 protects the privacy of student educational records and applies to all schools that receive funds from the Department of Education.

All users who have access to or may have access to personally identifiable student and user records shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Liberty County School Board Policies and Procedures, and all other applicable State and Federal laws and regulations, as they relate to the release of such information.

Below are the guidelines that must be followed where applicable:

- Encrypt data.
- Password protect data.
- Physically protect devices that can be easily moved such as PDA and Laptops that are used to access sensitive data.
- Avoid creating files that use social security numbers as identifiers. Use employee numbers and/or student local identification number instead.
- Never download or copy sensitive data to your home computer.

- Protect printed sensitive data. Store sensitive data in locked desk, drawer or cabinet. Do not leave unattended sensitive data on copier, FAX, or printer. Shred sensitive data that need to be disposed.
- Contact school administrator, department supervisor, or district administrator when questions arise regarding protected data.

4.3.2 Access and End User Support

Sensitive data access is restricted to only those personnel who need to perform their job duties. Access restrictions to such data are maintained by the IT Department in conjunction with the Finance Department, the Human Resources Department, the Superintendent of Liberty County School District, and the School Board. Access to sensitive information is only granted at the request of an administrator with an accompanying and verifiable need. Reviews of accesses and privileges are conducted twice per year and monitored to ensure compliance with all School Board Policies as well as State and Federal laws and regulations.

4.4 Guest and Vendor Access

- Guest and Vendor access will be granted through a Guest Portal which contains an electronic Guest Access Agreement that must be accepted before access is allowed.
- Using the Liberty County School District network is a privilege. As with all privileges, it is the responsibility of the guest user to use this service appropriately and in compliance with all school board policies and procedures, Florida state law, and Federal laws.
- The use of excessive bandwidth and reproduction of copyrighted materials is strictly forbidden and will result in the termination of network services.
- The Liberty County School District assumes no responsibility for costs associated with loss or damage to devices not owned by Liberty County School District while on the network.
- The Liberty County School District IT staff can only provide limited support in aspects of network connectivity and access of network resources.
- Backing up data and ensuring the security of network devices are the sole responsibility of the owner.
- Vendor supplied user ID's, program passwords, guest accounts, and security devices are administrated by the IT Department. This information and these devices are kept secure from general users unless knowledge of them is imperative to the course of their job.

4.5 User Laptop Policy

- Users will be responsible for the security of the laptop while assigned to them whether on or off campus.
- Users must understand that issued laptops are property of Liberty County School District and must be returned in their original condition upon request.

- Users assume all risk of injury or harm associated with the use of the laptop off-premises, including but not limited to, physical damage or loss, or personal injury.
- While laptops are being used off campus, the Liberty County School District has no control over the information accessed through the internet and cannot be held responsible for content viewed.
- Liberty County School District and its users will not be held liable for claims or damages that may arise from the use of issued laptops while not on school property.

4.6 Revocation of Privileges

Privileges and accesses to all Liberty County School District network devices, software, email, and information systems will be revised or revoked as necessary in the event of the following:

- Transfer of employee
- Resignation of employee
- Termination of employee
- Termination of consulting contract
- In the event of an investigation of employee, vendor, or consultant where revision or revocation of privileges and access is necessary.

5.0 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host, if that host is disrupting production services).

- Under no circumstances is an employee, student, or authorized guest of Liberty County School District authorized to engage in any activity that is illegal under local, state, federal or international law, while utilizing Liberty County School owned resources, to include the network and Internet.
- Users shall not access, download, store, send, or display text, images, movies, or sounds that contain pornography, obscenity, or language that offends or degrades others.
- Attempts to circumvent or defeat mechanisms put in place by the Liberty County School District staff to manage the network is strictly forbidden.
- Users shall not attempt to download and/or install services, electronic file sharing mechanisms, games, software, tools, or any executable file including but not limited to the following file types: .exe, .bat, .cmd, .zip, .msi, and .rar.
- Users shall not download or install unlicensed or unauthorized software on any Liberty County School District device or using the LCSD network to do so.

The list below is not exhaustive, it does, however, provide a framework for activities which fall into the category of unacceptable use.

5.1 Unacceptable Use: System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Liberty County School District.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Liberty County School District or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a Liberty County School District computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Liberty County School District account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning unless prior notification and approval is received beforehand.
- Executing any form of network monitoring unless prior notification and approval is received beforehand.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the user's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the network/Internet.

- Providing information about, or lists of, Liberty County School District's users to parties outside the Liberty County School District without prior permission from the Superintendent of Schools.

5.2 Unacceptable Use: Email and Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Students shall not use social network sites including, but not limited to, Instagram, Facebook, SnapChat, chat rooms, etc.
- Students shall not agree to meet with anyone met online.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Liberty County School District's networks of other internet/network service providers on behalf of, or to advertise, any service hosted by Liberty County School District or connected via Liberty County School's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

6.0 IT Administrator & Technician Responsibilities

It is the responsibility of the IT Technicians to follow the guidelines and policies of the Liberty County School District, Florida Department of Education, and all State and Federal Laws.

IT Technicians work with the Technology Coordinator. Training and meetings, as determined by the Technology Coordinator, are to be held between the IT Technicians and the Technology Coordinator in order to maintain close working relationships and openness in day-to-day communications.

Among their other responsibilities, the IT Technicians should use reasonable efforts to:

- Respond to requests for support, information, problem determination and problem resolution.
- Become familiar with all applicable Liberty County School District IT policies.
- Participate in required IT Technicians training and regular meetings as determined by the Technology Coordinator.

- Take precautions against theft of or damage to the system components and information.
- Comply with terms of all hardware and software licensing agreements applicable to the system.
- Treat information about, and information stored by, the network users in an appropriate manner and to take precautions protecting the security of the network and the security and confidentiality of the information contained therein.
- Promptly inform the Technology Coordinator of any computing incidents which clearly compromise network integrity, including but not limited to:
  - Notification by outside institutions or individuals of any incident.
  - Data loss or theft.
  - Inappropriate systems or information access or use
  - Any other breach or violation of IT policies of which they become aware.
  - Promptly notify the Technology Coordinator of material changes in network architecture or administration.

IT Technicians, when requested, are expected to cooperate fully with the Technology Coordinator in any investigation, identification, and resolution of network incidents.
IT Technicians are not responsible for the content of files, images, video or audio clips, electronic communications, and news postings produced by others. The IT Technician is also not responsible for unauthorized software installed by others. IT Technicians are responsible, however, for notifying the Technology Coordinator of any observed violations of Liberty County School District policies, licensing agreements with software manufacturers, or observed violations of local, state, or federal laws regarding these matters.

7.0 Security Incidents

7.1 Definition

A security incident is any violation of set Policies and Procedures that may or may not result in the following:

- loss of information confidentiality (data theft)
- compromise of information integrity (damage to data or unauthorized modification)
- theft of physical IT asset including computers, storage devices, printers, etc.
- denial of service
- misuse of services, information, or assets
- infection of systems by unauthorized or hostile software
- an attempt at unauthorized access
- unauthorized changes to organizational hardware, software, or configuration
- reports of unusual system behavior etc.

7.2 Response

If an IT Technician becomes aware of a security incident, they must provide notification of the incident to the Technology Coordinator. Upon confirmation, the Technology Coordinator will notify the user's supervisor (if a Liberty County School District employee) or School Administrator (if a Liberty County School District student).

Other steps that may be taken:

- Temporarily suspend or restrict the user's computing privileges during the investigation. Reactivation is at the discretion of the appropriate administrator.
- Remove the affected computer device, as appropriate, from the network.

These steps may be taken only after authorization by the Technology Coordinator unless the situation represents an emergency or immediate threat to network security/integrity. In such case, the IT Technician must take corrective action and notify the Technology Coordinator as soon as possible. Actions should be taken in such a way that any impacts to non-offending users are minimized.

7.3 Monitoring

7.3.1 Devices and Applications

In effort to maintain network security, integrity, and to reduce the risk of Security Incidents the IT Department can and will monitor network activity. These monitoring devices/applications may include but are not limited to:

- Firewall logs
- Web Filtering logs
- Network Traffic Monitoring
- Active Directory Monitoring
- Mail Scanner logs
- Database, backup, and usage logs on servers
- Event logs and histories created in individual machines

7.3.2 Files and Correspondence

In the course of their duties, it may be necessary for IT Technicians to view files, data or communications that have been stored by users on devices or network file servers. The viewing of such material is permitted only when it is necessary to troubleshoot problems at the request of the user, protect the security and integrity of the Liberty County School District's network, protect the rights or property of Liberty County School District or third parties, or to ensure compliance with Liberty County School District policy or applicable law. Examples include:

- The identification/restoration of lost, damaged or deleted files;

- The identification of a process that is interfering with normal network functions;
- In more serious circumstances, an investigation of a Security Incident.

In all such cases, the IT Technician shall take into consideration the confidential nature of files and/or communications that may potentially be reviewed and shall implement the appropriate safeguards to ensure that all local, state and federal privacy laws are complied with. The Technology Coordinator must be advised of and approve any non-routine monitoring that occurs. Non-routine monitoring includes directed investigations of potential policy and/or security violations. Discovery of such violations in the course of routine monitoring must be reported.

8.0 Data Loss Prevention

To prevent data loss from a disaster, the IT Department will follow all disaster policies and guidelines set forth by the Liberty County School District. In addition, the IT Department will take routine measures to protect and restore data on-site systems by performing backups and storing backups. Contracts for information systems off-site include data Joss protection plans and disaster recovery plans as a rule before approval.

In the event of immediate threat, the IT Department will take the following actions:

- Backups will be performed and stored in multiple locations if possible
- Most servers except mission critical servers (Active Directory) will be shut down.
- Information will be provided on the Liberty County School District web site.
- Network closets and battery backups (UPS) should be turned off if unnecessary
- In the event the MIS building is damaged or destroyed, operations will be re-established at one of the schools or department buildings or a neighboring county within the PAEC group.

Each school and district office department should take the following steps to protect data and equipment:

- Computers should be turned off and unplugged, if connected to battery backups there should be turned off and unplugged as well.
- Computers should be moved away from windows, off the floor, and covered with plastic if possible.

9.0 Purchasing

The IT department is responsible for the seamless integration of any hardware or software into the existing network system. When considering the purchase of any technology related item, prior approval from the IT Department is required.

10.0 Disposal of Technology Equipment

All technology equipment must be disposed of in a manner that adheres to all State and Federal Laws as well as Liberty County School Board Policy.

11.0 Enforcement

Failure to adhere to these policies and guidelines may result in suspension or revocation of the offender's privilege or access to the network and/or other disciplinary or legal action.

12.0 Revisions

The Liberty County School Board reserves the right to change these policies and procedures at any time to ensure the operability and safety of the network and its users.