



SUMMIT

ACADEMY

EMERGENCY PROCEDURES GUIDE

2026-2027

INTRODUCTION AND USE OF THIS GUIDE

Summit Academy SC works cooperatively with its sister schools Youth Leadership Academy (YLA) and Tall Pines STEM Academy (TPSA) as well as local government and community agencies to prevent, assess, manage, and follow-up on any threat to the safety of the students, faculty, or staff. This guide is designed to contain the primary elements or steps necessary for effective intervention and follow-up for selected common emergencies that affect our school.

Since the enumeration of all emergency situations that might occur in the future is not possible, this guide, and the school's detailed emergency manual, along with the exercise of good judgment should help to ensure that emergencies will be managed effectively. All school faculty, staff and appropriate government and community agencies have access to the guide. The school staff will be trained in the use of this guide.

Stakeholders: Summit Academy SC board is involved in the process of approving the safety and emergency plan.

PREPARATION IS THE KEY TO SUCCESSFUL EMERGENCY MANAGEMENT

Preparation for an emergency is just as vital as the rapid and effective response and recovery from the emergency. It is vital that administration, staff and students be equipped with the information and training to deal with any type of emergency situation.

The following are some of the necessary steps to effective preparation for any situation that disrupts routine activities on campus.

- 1) A "Grab and Go" kit is a vital part of your school's emergency management capability. The Grab & Go kit must be taken with the Administrator in charge for all practice, actual or potential evacuation scenarios.
- 2) Exercising of emergency plans, through either drills or administrative "tabletop" exercises will be conducted to aid in identifying weaknesses. Tabletop exercises will be either a step-by-step discussion of how staff would respond to a particular situation, or a brief brainstorming session centered around "what problems would this situation present and how do we overcome them?"

SUMMIT ACADEMY SC

EMERGENCY PROCEDURES

TABLE OF CONTENTS

EMERGENCY COMMUNICATIONS INFORMATION	A
ASSESSING THE SCHOOL CRISIS	B
FIRE	C
BOMB THREAT AND EXPLOSION	D
SEVERE WEATHER	E
CHEMICAL / BIOLOGICAL / NUCLEAR	F
HAZARDOUS MATERIALS	F
EARTHQUAKE / UTILITY EMERGENCY	G
CRIME REPORTING	H
STUDENT DISTURBANCE	I
CAMPUS INTRUDER / SUSPICIOUS PERSON	J
STUDENT RUNAWAY / ABDUCTION	K
WEAPON ON CAMPUS	L
DEATH OR SERIOUS INJURY BY VIOLENCE	M
HOSTAGE SITUATION	N
COMMUNICABLE DISEASES	O
ACCIDENT / SERIOUS ILLNESS / INJURY	P
STUDENT HEALTH AND MENTAL HEALTH	Q
OFF CAMPUS EMERGENCY – PRE-PLANNING	R
OFF CAMPUS EMERGENCY – ACTION STEPS	R
MEDIA PLAN	S
EMERGENCY EVACUATION	T
STUDENT/PARENT REUNIFICATION PROCEDURES	U
ACCESSIBILITY AND SPECIAL NEEDS ACCOMMODATIONS	V
SAFETY COMPLIANCE FOR PARTNER FACILITIES	W
ROUTINE SAFETY INSPECTIONS & ANNUAL TRAINING	X
SCHOOL OPERATIONS	Y
COMMUNICATION PROCEDURES	Z
YLA/ CULI CAMPUS SITE MAP (PICKENS, SC)	AA
CAMP LONG/ TPSA SITE MAP (AIKEN, SC)	BB

A - EMERGENCY COMMUNICATIONS INFORMATION

Administration Offices:

Summit Academy 698 Concord Church Rd; Pickens, SC 297671
Main Office: 803-291-0040

Youth Leadership Academy 698 Concord Church Rd; Pickens, SC 29671
Main Office: 864-898-4511
Office Fax: 864-878-5985

Tall Pines Academy 82 Camp Long Rd; Aiken, SC 29805
Main Office: 803-502-1692

<u>Administrators</u>	<u>Office</u>	<u>Mobile</u>
Director of Schools, YLI	864-898-4511	864-430-5999
Principal		864-321-3445
Instructional Coach		864-320-3111
Office Manager		864-508-4266
Special Projects Coordinator		864-423-9953
SRO (YLA)		864-918-1547
SRO (TPSA)		803-502-1692

EMERGENCY COMMUNITY SERVICES

<u>Agency</u>	<u>Phone</u>
----------------------	---------------------

ALL EMERGENCIES

Fire / Law Enforcement / EMS	911
------------------------------	------------

Hospitals

AnMed Cannon Memorial Hospital (Pickens, SC)	(864) 878-4791
Prisma Health Baptist Easley Hospital (Pickens, SC)	(864) 442-7200
Aiken Regional Medical Center	(803) 641-5000

Other Agencies

Pickens Police Department	(864) 878-6366
Pickens County Sheriff's Office	(864) 898-5500
Aiken County Sheriff's Office	(803) 648-6811 or (803) 642-1762
Aiken County Emergency Management Division	(803) 642-1623
American Red Cross (Pickens, SC)	(864) 878-0131
American Red Cross (Aiken, SC)	(803) 641-4152
CSX Transportation Police Department	800-232-0144
National Response Center (Toxic Chemical)	800-424-8802
DHEC	803-253-6488

B – ASSESSING THE SCHOOL CRISIS

In order to effectively manage a school emergency, some determination must be made by the Principal or the School Crisis Response Team as to the magnitude and intensity of the situation so that appropriate resources can be mobilized. The school uses a three-level system for this purpose.

Considerations to be used in determining crisis level:

1. Degree of life threat and/or danger
2. Amount of loss (family, friends, classmates)
3. Immediacy of crisis
4. Duration of trauma
5. Amount of damage or destruction to possessions, homes, or community
6. Potential for further crisis
7. Exposure to death and destruction
8. Amount of moral conflict (e.g., controversial issues)
9. Individual(s) affected (victim, perpetrator, witness)
10. Number affected by trauma
11. Possible long-term effects
12. Degree of “rumor” potential in media coverage

Level I: Essentially a day-to-day crisis which will be handled by the school administration and/ or the School Crisis Response Team. Any doubt concerning the level of the crisis at any time during or after the onset of the crisis will be resolved in cooperation with the District Office. Where only notification is required, the school will use an appropriate communication format (telephones, fax, letter, etc).

Level I (In-house)

Notification to District Office

Student fight or disruptions	No
Heavy vandalism (property damage)	Yes
Accidents involving students and staff	Yes, if medical treatment
Disruptive intruders	Yes
Lost or runaway students	Yes
Bomb threat	Yes
Death of student	Yes

Death of faculty or staff member Yes

Kidnapping by unauthorized parent Yes

Weapons on campus Yes

Sexual Assault Yes

Level II: Essentially a school crisis which will include the involvement of at least the district office supervisor, the school crisis response team, and possibly the district crisis response team. Immediate notification of the District Office is necessary.

Serious accidents at school or off-campus

Disruptive intruders

Violence with weapons on campus where crime or personal injury results

Lost or runaway students

Death of student(s) or staff at school

School fires

Kidnapping

Extended utilities cutoff

Assault of faculty or staff member

Explosion

Catastrophic illness

Sexual assault

Weapons on campus

Level III: Essentially a full-blown crisis which will require the assistance of the District Office Crisis Response Team and the involvement of law enforcement, emergency preparedness, and other appropriate government and community agencies. Immediate notification to the district office is imperative!

Natural disaster (tornadoes, etc.)

Serious accident (multiple or serious injury)

Suicide or homicide of student or staff during school day on school property

Traumatic national disaster (e.g., death of President)

Poisoning or chemical spills

Bombs, explosions

Hostage situations

CRISIS PREPARATION:

For preparation to meet a crisis at any level, the following items should be assembled and be available prior to the onset of any disrupting event:

1. List of approved counselors or aftercare providers who can be called on for assistance.
2. Communication plan for faculty, students, and parents, including death notification procedures, etc., and the means to be used for communication.
3. This emergency document with emergency procedures and phone numbers.
4. An assessment process, (e.g. who is going to investigate the incident and a means to assess who may need help.)

ACTION STEPS:

1. Investigate the crisis fully.
2. Determine who is affected physically and psychologically.
3. Determine the type and level of the response needed
4. Activate resources and make a schedule to use resources to meet the identified need.
5. Keep the faculty informed of actions taken.
6. Evaluate the response to determine if the identified needs were met by the counseling, debriefing, or activities that were used.

C – FIRE PROCEDURES (LEVEL II OR III)

In the event of a fire within the school building:

- Sound the fire alarm immediately.
- Notify the fire department by calling 911 and Notify the SRO.
- Provide important details including possible breaks in gas or electrical lines or other special hazards
- One staff person will be designated to meet the first responder.
- The designated person will provide a master key or keys to the first responder.
- Staff person will carry a portable radio, school floor plan, and will stay with the first responder

Evacuate the building according to the following procedures:

- Students will walk out of the designated exit in a quiet orderly manner. Each teacher should check the classroom and be the last individual to leave.
- Teachers will take their class lists of students as they exit the classroom.
- Teachers will close windows and doors.
- In each class, the student reaching the outside door first will hold it open for the others.
- Students must go to a designated area that is a safe distance from the building and must not stand in any driveway or other hard surfaced area close to the building. Evacuation may require students to leave school property.
- Students not in the classroom when the alarm sounds should report to their teacher's designated area outside of the building. No one should enter the building when the alarm sounds.
- Teachers are responsible for students and their supervision and should take attendance, accounting for each child. A child not accounted for is to be reported to the Principal/Assistant Principal immediately.
- The fire drill plan for evacuation is posted in each classroom. It is the teacher's responsibility to be thoroughly familiar with the plan and also be prepared to use an alternate route in the event the normal route is blocked.
- Access roads will be kept open for emergency vehicles. Principal WILL have designated an individual or group of individuals to ensure that all access roads are open.
- Students and staff members will be allowed to return to the building at the direction of the principal only upon the recommendation of the Fire Department.

Fire extinguisher locations:

YLA/ CULI - Every classroom and office has at least one fire extinguisher. These are located on an internal wall next to one of the main entrances/exits. TPSA/ Camp Long - YLA/ CULI –Classrooms, Cabins and office have at least one fire extinguisher. These are located on an internal wall next to one of the main entrances/exits.

***Every school must determine evacuation sites with the fire department personnel. Each school must identify an alternate evacuation site.**

D – BOMB THREAT AND EXPLOSION PROCEDURES

Definition Bomb Threat: Bomb Threat: S.C. State Law (16-23-750) a person who communicates a threat or conveys false information, knowing the information to be false, concerning an attempt or alleged attempt of an explosive device is guilty of a felony and upon conviction must be imprisoned for not less than one year nor more than ten.

Action Steps for Bomb Threats:

PORTABLE RADIOS AND CELLULAR PHONES SHOULD NOT BE USED IN THE IMMEDIATE VICINITY OF A SUSPECTED DEVICE DURING A BOMB THREAT INCIDENT.

We must be able to maintain communications during a bomb threat incident. **DO NOT** transmit in the immediate vicinity of a suspected device. Move away from the area before using cell phones or radios.

If a phone threat is made, obtain as many details as possible. Use the checklist that follows: COMPLETE THE PHONE CHECKLIST. USE CALLER ID FUNCTION UPON COMPLETION OF CALL.

Call 911 to notify police, fire department, and emergency preparedness. Follow the steps of the Annoyance Call Tracing System.

When the Principal decides to evacuate the building, the special code for a bomb threat must be announced on the intercom prior to activating the fire alarm system. Normal fire alarm procedures should be followed after the fire alarm sounds.

The building should be left as is. Students are requested to take their backpacks/ book bags with them as they exit the building.

Notify District's Director of Special Services.

Staff should be aware of unusual or suspicious boxes, packages, noises, devices, or disturbances in their classroom or in the hallway as they evacuate the building **do not touch anything that looks suspicious. Report suspicious items to the principal.**

The school will be searched by school personnel with assistance from security personnel and law enforcement according to a plan developed by the school. The principal, law enforcement and security personnel will consider the time indicated by the caller to determine when the building will be searched.

Stay in a safe designated area until the principal indicates it is safe to return to the building. Students should be faced *away* from the building and be prepared to drop to the ground in the event of an explosion. Teachers should check the assembly area for the possibility of secondary devices.

If an explosion occurs prior to evacuation, teachers should be prepared to move in a darkened, smoke filled and disruptive environment. Teachers should lead the *way* and students should physically grasp the student in front of them.

Upon reaching the assembly area, Teachers should immediately account for all students and report

any missing to staff and/or emergency personnel.

***Every school must determine evacuation sites with fire department personnel. Each school must identify an alternate evacuation site.**

Bomb threat Call Checklist:

1. When is the bomb going to explode? _____
2. Where is the bomb going to explode? _____
3. What does the bomb look like? _____
4. What kind of bomb is it? _____
5. What will cause the bomb to explode? _____
6. Did you (the caller) place the bomb? _____
7. Why did you (the caller) place the bomb? _____
8. Did you (the caller) make the bomb? _____
9. What is your name? _____
10. Where do you live? _____

Caller information: Male / Female Age: _____ Race: _____ Length of call: _____

Caller's Voice:

Calm	Laughing	Lisp	Angry	Crying	Rasp	Excited
Normal	Deep	Slow	Distinct	Ragged	Rapid	Slurred
Soft	Clearing Throat	Nasal	Deep Breathing	Loud		
Stutter	Cracking Voice	Disguised	Accent	Familiar		

If familiar, who did it sound like? _____

Background Sounds:

Street Noise	House Noises	Factory Machinery	Crockery	Motor	Animal Noises
Voices	Office	Clear	PA System	Static	Local
Long Distance	Office Machinery		Booth	Other	

Threatening Language:

Well Spoken	Foul	Incoherent	Irrational	Taped
-------------	------	------------	------------	-------

Remarks:

Report call immediately. Fill form out completely. Note date and time.

BOMB / EXPLOSION

STEPS OF ACTION FOR EXPLOSIONS:

- Determine location and extent of explosion.
- Call 911 and provide important details regarding possible breaks in gas and electrical lines or other special hazards.
- Evacuate buildings using normal evacuation procedures when all flying debris ceases. Special conditions may warrant special instructions to use alternative exits.
- Custodian will shut off gas.
- Assist with injured or wounded.
- Notify District's Director of Special Services.
- Secure the area until authorities arrive.
- Send one person to meet the emergency first responder to explain the situation. This person should carry master keys, floor plan, and walkie-talkie.
- If an explosion occurs prior to evacuation, students should seek cover under their desks, if possible. At all times they should cover their heads with their hands and take a kneeling face down position on the floor. They should stay in this position until flying debris ceases.

*** All persons should be alert to the potential for secondary explosions.**

E – TORNADO, SEVERE THUNDERSTORM, HURRICANE PROCEDURES

(Level I - Warning, Level III - Strike)

Tornadoes and severe thunderstorms can occur suddenly; therefore, the following precautions and procedures shall be used.

Definitions:

Tornado Watch: Conditions are favorable for tornadoes or severe weather. Make staff aware but take no action.

Tornado Warning: Tornado has been sighted - take shelter immediately.

Severe thunderstorms, tornado watches and tornado warnings will be indicated to school buildings over the tone alert radios in school offices. Radios must be left on at all times.

The warning signal (or tornado drill) will be by either: The public address system.

If the electricity is off, teachers will be notified by a runner or by walkie announcement.

Action Steps

- To signal a tornado warning or severe thunderstorm, an announcement will be made that the following steps should be taken.
- Students should proceed to their designated positions against the wall and assume a kneeling position, head down, with hands covering their heads.
- Students in unsafe locations at the time of the drill will go to assigned locations at the direction of the Teacher.
- Teachers are to close classroom doors after students exit into the tornado safe area.
- Quiet is extremely important so that any necessary directions may be heard in the tornado safe area.
- Teachers should keep their class rosters with them during the drill to verify student classroom count. They should kneel behind their classes to be sure students are following the drill or emergency procedure.
- The all-clear signal will be a verbal command or announcement by the principal or designee.

***During a tornado warning, all portable buildings will be evacuated to a permanent structure.**

Other Procedures

- In an outside office, blinds are to be closed on windows and office personnel are to use telephones in the inner office away from glass windows/areas.
- During a tornado watch, a weather spotter (designated person) is to be posted in an area listening to local weather communications.
- The alert monitor should be located within hearing distance of office personnel.
- In the event of a tornado sighting, the school office will contact 911.

Action Steps for Severe Thunderstorms:

- Upon notification of a violent storm, a spotter should be tracking the storm.
- The principal should notify all teachers and students to be in the school building and not outside of the building during a severe thunderstorm.
- Teachers and office personnel should close all windows and blinds.
- Students and teachers should move away from glass/window areas during a violent storm.
- If a severe thunderstorm strikes the school, all students and teachers should move to the tornado safe area for protection from electrical hazards and flying debris. Assume the face down, kneeling position for safety.
- Contact 911.
- Stay in the face down position until all clear signal is given by the Principal or emergency personnel.

F – Chemical / Biological / Radiological (CBR)

With regard to concerns about a CBR attack, we would follow the procedures listed below in the event of an attack in our area:

- Go to lock down. Secure all doors and windows.
- If interior rooms are available, move to them.
- Air handling systems should be shut down on site or remotely by Support Services.
- Stand by for announcements from the DO, SSC and civil authorities. There are variables in these types of attacks, and it will be best to shelter in place until we have better information. Parents should be advised not to come to the school to pick up their students until an all clear is given

HAZARDOUS MATERIALS INCIDENT (Level II or Level III)

Hazardous materials near the school could pose a serious threat to the safety of students and staff. Immediate communication with local emergency preparedness, fire, and police is necessary.

Signals:

- A) Notify the SRO
- B) Tell students/staff what is occurring and why; or
- C) Notify all staff outlining and explaining the emergency and whether school is to continue as usual, or people are to evacuate to another location if necessary.

Hazardous Materials Threats Action Steps:

- Identify threats to school.
- Contact 911 Emergency Services to notify them about the incident. Provide appropriate details of the incident and chemical code number, if visible. Chemical codes are listed in the Emergency Response Guidebook available through the Emergency Preparedness Office.
- Determine whether to maintain school or evacuate buildings.

Follow the directions of the Fire Department and emergency personnel as to appropriate steps in terms of evacuating the building.

In-Building Chemical Hazards:

When hazardous chemical accidents occur in the school building, personnel will follow the accident control procedures established in the plan for our school. These plans are housed in the school's office and are readily available.

G – EARTHQUAKE PROCEDURE

Signals: Announcement on school intercom system to assume duck, cover and hold position.

Action Steps:

- Protect face and head from flying debris with arms, books, coats, etc. Duck, cover, and hold procedures should be used.
- Stay in this position until building tremors and/or flying debris ceases.
- If directed to evacuate the building, you should move to an area on the school campus that is not located near gas and electrical lines that could pose a hazard if broken.
- Contact 911 and provide details of building damage and emergency needs.

***Plan for alternate routes to evacuate buildings during earthquake drills. *Do not light any matches or candles if an earthquake occurs.**

UTILITY EMERGENCY PROCEDURES (Level II or Level III) Signals:

If the building needs to be evacuated, follow fire drill procedures with a verbal announcement on the school communication system, followed by manually tripping the fire alarm. If there is an emergency due to an electrical failure, a verbal announcement will be made by a runner. A visual check of all school areas will be conducted by the Principal, Custodian, and other designated staff.

Action Steps:

Gas Line Break - Call 911 & notify the SRO - Inform of break and important details.

- Clear the area (evacuate the building, if necessary).
- Teachers should account for all students on their attendance rolls. Report missing students to the principal.

Electrical Power Failure - Call 911 & Notify the SRO

Clear the immediate area of obvious hazards (evacuate building, if necessary)

Teachers should account for all students on their attendance rolls. Report missing students to the principal.

Water Main Break or Sewer Break - Call 911 & Notify the SRO. Provide details of the type break.

Clear the immediate area of obvious hazards (evacuate the building, if necessary).

Call the appropriate water company and provide details.

H – CRIME REPORTING PROCEDURES

AGAINST PERSONS/PROPERTY (Level I, II, or III)

These are enforcement procedures which are required by law, to be followed in the instance of suspected criminal conduct.

When an administrator observes (or is notified of and verifies) an offense, the administrator will confer with the staff involved, notify the SRO, effect the appropriate disciplinary action, and if appropriate, meet with the student. If warranted, the administrator should immediately remove the student from the school environment. The administrator will notify a parent/guardian as soon as possible.

When appropriate, school officials should contact law enforcement authorities.

If law enforcement is notified, the District's Director of Special Services.

Staff will follow established due process procedures when applicable.

The administrator will keep a complete record of the procedures.

South Carolina State Law (SC Code Sec. 59-24-60, as amended March 1994) requires as follows:

“In addition to other provisions required by law or by regulation of the State Board of Education, school administrators must contact law enforcement authorities immediately upon notice that a person is engaging or has engaged in activities on school property or at a school-sanctioned or sponsored activity which may result or results in injury or serious threat of injury to the person or to another person or his property as defined in local board policy. Specifically, the actions which will result in the immediate contact of law enforcement include, but are not limited to the following:

- assault and battery
- extortion
- bomb threat
- possession and/or use of and/or transfer of a weapon, including a pistol, knife, blackjack, brass knuckles (to include multi-finger rings);
- possession of incendiary or explosive devices, including ammunition for a weapon, such as bullets, shotgun shells, etc.
- In addition, any item used to inflict physical harm on another person will be considered a weapon.
- sexual offenses
- vandalism (major property damage)
- theft, possession, or sale of stolen property
- arson
- furnishing or selling unauthorized substances, as defined by Board Policy.
- distribution, sale, purchase, manufacture, use or unlawful possession of a controlled substance (a drug, substance, or an immediate precursor as defined in South Carolina Code of Laws Section 44- 53-190 through 44-53-270)
- threatening to take the life of or inflict bodily harm upon school personnel, school volunteers, or members of their immediate family
- possession, use, or transfer of “look-alike” weapons.
- disturbing the schools

I – STUDENT DISTURBANCE PROCEDURES

Student Disturbances:

If the misbehavior is not serious, attempt to have students return to their normal school routine.

Call for the SRO if the disruption continues or if injury occurs.

If the SRO needs more assistance and local law enforcement is notified, call the District's Director of Special Services.

If the behavior could result in injury or further disruption, try to get disruptive students or their leaders isolated from the general student body.

Determine what disciplinary action to take, if any.

Notify parents at an appropriate time.

School Crisis Response Team members discern the basis for the problem and take action to address those concerns.

Student Walkout Procedures

- Assign administrative security.
- Advise Law Enforcement
- Activate the School Crisis Response team to discuss the problem and take action to address the situation.

J – CAMPUS INTRUDER (Level I)

Definition: Individuals who do not receive permission from the school office to be on the school premises

General procedures - Staff should stop strangers and inquire as to their business in the building. Contact the office to be sure they have registered. All strangers should be provided identification badges when they sign in at the office. Use PA to notify teachers of unwanted intruders in the building. Teachers should lock their classroom doors immediately. All staff will participate in ALICE training. ALICE training will also be offered to students.

Action Steps:

- If the intruder is in the school, staff should use two-way intercom to report to the office, if possible.
- If use of the intercom is not possible, ask the intruder if you may be of assistance and communicate in a non-threatening manner until help can be sent.
- Ask unwanted intruders to report to the school office. If the intruder refuses to report to the office the teacher should contact the office and advise of the situation and give a description of the intruder.
- Staff should escort strangers to the office if determined to be non-threatening.
- If in the classroom, Teacher should seek assistance from the office.
- If the intruder is hostile or threatening, call the school office for assistance. The school office should contact law enforcement for assistance.
- If the intruder becomes violent, the Teacher should notify the school office by using the code blue for intruder in the building. The school office should use the intercom to notify all classrooms. The school's special code blue should be used when notifying all teachers and staff.
- If shots are fired, the intercom or bullhorn will be used to evacuate students to the safest position away from intruders. Otherwise, students should be in the classroom and the classroom door should be locked, to prevent entry by an intruder.
- Notify the District's Director of Special Services.

Reminders:

- Schools have the right to search all individuals on a school campus or on school buses and should have posted signs at the entrances to advise visitors of this law.
- All visitors on the school campus must report to the office to sign in.
- All visitors must be provided a visitor's badge before being allowed to leave the school office.

Emergency Drills for Lock Down Procedures

Authority to call drills: The sounding of an alarm for the purpose of a drill or a lock down is an authority possessed solely by the principal or his or her designee.

Purpose: These drills are conducted to familiarize the occupants of a building with the signals and lockdown procedures so that in case of emergency there shall be no hesitation or confusion in directed student action. These drills are for the safety of all persons involved, and each person must realize that the success of the drill is dependent upon his/her actions and cooperation. Therefore:

- All persons in the building must take part in the drill.
- Every alarm should be considered as a warning of an actual emergency.

Frequency of Drills: There shall be a minimum of two (2) drills per school year. The first drill shall be conducted within fifteen (15) days of the first day of school. The second drill shall be conducted at the principal's discretion.

Warning Signal: The warning signal shall be "Intruder on campus." There should also be a plan for signaling in the event of power failure.

Responsibilities of Principals: Principals shall:

- be responsible for all matters pertaining to organizing and conducting drills on the campus and for the efficiency of the drill and corrective actions taken for violation of the rules and problems identified during the drill;
- Appoint a subordinate staff person to supervise particular areas of need and instruct him/her in the general plan for lock downs and details of his/her specific duties, such as instruction regarding:
- how to send an alarm to the Sheriff's Department, including how the alarm system operates, both electrical and emergency;
- the importance of quick action in sending an alarm;
- how to secure all building exits;
- which building location shall be the command center when a lockdown is in progress; and
- what method of communication shall be used if an intruder is in the building before lock down can be established;
- be prepared to direct first responders to incident location and give them any necessary information;
- ensure that teachers and students perform all activities assigned to them during the event;
- notify the Director of Student Services (803-734-8067 or 803-230-9593 (c)).
- Designate an administrator or staff person to coordinate with public safety personnel at their command post; and make sure a site map and keys are available.
- Be prepared to deal with parents and media who respond to the school.

Responsibilities of Teachers: Teachers shall:

- be in charge of their respective classes;
- issue all commands relative to participation in the drill;
- ensure proper lock down procedure;
- keep students in a safe area until advised personally by administration or public safety personnel to move or that the all clear has been given;
- be prepared to lead their class to designated secure areas.
- students shall walk briskly (do not run) without talking or breaking from the line.
- teachers shall check roll when the assigned area is reached.
- teachers shall notify the principal immediately of any missing student
- teachers shall not leave the students unless they are relieved by an administrator.

During Lock Down Drills: Building staff shall follow the directions laid out in YLA's/ TPSA lock down plan when using those campuses.

Type of Lock Downs

- **LOCK DOWN:** This is a total lock down of the facility. All exits are secured. Classrooms are locked and only necessary staff movement is allowed until the incident is resolved.
- **MODIFIED LOCKDOWN:** Exits are secure, and staff will monitor until the incident is resolved. Normal classroom schedule will continue.

After a Lockdown Drill: Principal and staff shall meet to evaluate effectiveness of the drill and make possible changes.

K – STUDENT RUNAWAY OR ABDUCTION (Level I or Level II)

Definition: Student runs away from the school building during school hours, or student is abducted by a stranger or family member.

Action Steps:

- 1) The teacher or staff member should notify the school office, SRO, and provide a description of the student(s) and abductor(s) and as much information as possible about the incident.
- 2) The school office personnel should call 911 for an abduction or for a runaway. Provide a description of the persons involved and as much information as possible about the incident.
- 3) For a runaway, follow the student if it seems appropriate.
- 4) School office personnel should contact the parent or guardian.
- 5) Have a description of student's clothing worn that day and a picture of the student available for law enforcement personnel. Check with teachers to obtain clothing description and surveillance systems. Pictures may be available from files or yearbooks, but a picture of every student must be available!
- 6) Notify the District's Director of Special Services

L – POSSESSION OF WEAPON ON CAMPUS

Whenever a student is observed or reported to have a weapon on campus, the following precautions and procedures should be followed by the school administrators and/or staff:

- 1) Any person found to be in possession of a weapon should be reported to the school office, and SRO. Identify the person and his/her location in the building.
- 2) Communicate with the appropriate staff of the weapon.
- 3) Contact law enforcement for possession of a weapon. If there is a threat to life or property, call 911. Person calling 911 should clearly identify the nature of the threat.
- 4) Notify the District's Director of Special Services.

M – DEATH OR SERIOUS INJURY ON CAMPUS (Level III)

Whenever a student, staff member, or visitor on campus is seriously injured, the following procedures should be followed:

- 1) Notify 911, notify the SRO, and provide details of the incident. Request law enforcement and emergency services. Provide 911 with all details of the incident
- 2) Determine injuries and provide first aid.
- 3) Restore calm and move students away from the scene. Students should not be allowed to leave class to go to the scene.
- 4) Fax or send medical emergency information to hospital on victims.
- 5) Assess the extent of the situation by determining who was involved or committed the act. Identify witnesses and remove them to a secure area. Keep witnesses separated. Keep the scene a secure area. Do not disturb possible evidence or remove the victim if determined to be dead.
- 6) Notify the District's Director of Special Services.
- 7) Follow emergency procedures for communication of information to staff and students, evacuate (if necessary).
- 8) Follow crisis response follow-up plan for necessary counseling or other trauma reduction activities.

N – HOSTAGE SITUATION PROCEDURES (Level III)

If a situation should arise where one or more persons hold students or staff hostage on the campus, the following precautions and procedures should be considered:

- 1) Call 911 and notify SRO.
- 2) Move all people away from the hostage situation as rapidly and quietly as possible. Check any common areas to be sure they have been evacuated.
- 3) Gather all facts regarding the situation for the police. Keep notes on times, any communications from the person holding the hostage, and other witness information.
- 4) Designated first responders should meet law enforcement and emergency personnel as they arrive on campus.
- 5) Work with the district office and law enforcement to determine next steps. Law enforcement has total control of hostage scene
- 6) Notify the District's Director of Special Services.

* Note: No one, other than law enforcement, should initiate communication with the subject. If communication is initiated by the subject, only one person should communicate with the subject.

O – COMMUNICABLE DISEASES (Level I or Level II) Guidelines for Handling Body Fluids in Schools

Does contact with body fluids present a risk?

The body fluids of all persons should be considered to contain potentially infectious agents (germs). The term body fluids includes: blood, semen, drainage from scrapes and cuts, feces, urine, vomitus, respiratory secretions (e.g., nasal discharge) and saliva. Contact with body fluids presents a risk of infection with a variety of germs. In general, however, the risk is *very* low and dependent on a variety of factors including the type of fluid with which contact is made and the type of contact made with it.

What should be done to avoid contact with body fluids?

When possible, direct skin contact with body fluids should be avoided. Disposable gloves should be available for custodians, nurses, and others who come in contact with body fluids. Gloves are recommended when direct hand contact with body fluids is anticipated. Hands should be washed after gloves are removed and gloves discarded in a plastic bag.

What should be done if direct skin contact occurs?

Hands and other and other affected skin areas should be washed with soap and water. Clothing non-disposable items that are soaked with body fluids should be placed in plastic bags. Disposable items should be handled as with disposable gloves.

How should spilled body fluids be removed from the environment?

Schools should stock absorbent agents specifically intended for cleaning body fluid spills. Disposable gloves should be worn when using these agents. The dry material is applied to the area, left for a few minutes to absorb the fluid, and then vacuumed or swept up. The vacuum bag or sweeping should be disposed of in a plastic bag. Broom and dustpan should be rinsed in a disinfectant.

Hand washing procedures

Proper hand washing requires the use of soap and water and vigorous washing under a stream of running water from ten seconds to a minute. Use paper towels to thoroughly dry your hands. An intermediate level detergent, disinfectant of Clorox 1:10 solution should be used to clean surfaces contaminated with body fluids.

Disinfection of hard surfaces and care of equipment

After removing the soil, a disinfectant is applied. Mops should be soaked in the disinfectant after use and rinsed thoroughly or washed in a hot water cycle before rinse. Non-disposable cleaning equipment should be thoroughly rinsed in the disinfectant. The disinfectant solution should be disposed of down a drainpipe.

Disinfection of rugs

Apply sanitary absorbent agent, let dry, and vacuum. If necessary, mechanically remove with dust pan and broom, then apply rug shampoo (a germicidal detergent) with a brush and re-vacuum. Rinse the dustpan and broom in disinfectant.

P – ACCIDENT/SERIOUS INJURY/ILLNESS PROCEDURES (Level I, II, or III)

Definition: Emergency where one or many are sick or injured. Immediate concern is to aid the injured or sick student.

Signals: Use Public Address system.

Action Steps:

- 1) Teachers should contact the school office and stay with injured/sick people.
- 2) School offices should contact 911 if an individual's injury or sickness is determined to be of a nature that should be treated immediately by a medical doctor. First priority is the safety and well-being of the individual.
- 3) Fax or send medical emergency information to the hospital with the victim.
- 4) If a qualified individual is available to administer first aid, use him/her as appropriate until emergency personnel arrive on the scene.
- 5) Contact the individual's parent/guardian to notify him/her of the emergency, to advise of the decision to transport for emergency care and request the parent/guardian to go to the child's location.
- 6) Notify the District's Director of Special Services

Note: Use universal precautions when handling body fluids.

First Aid and Emergency Supply Locations:

Each classroom has a first aid kit and a stop the bleed kit located inside the room. If additional supplies are needed, they are located at the nurses office.

Q – STUDENT HEALTH AND MENTAL HEALTH

1. Suicide Prevention & Response Procedures

To ensure student safety, all reports or observations of a student expressing self-harm or suicidal ideation must be addressed immediately and strictly followed according to the protocol below:

- **Immediate Notification:** Any staff member who becomes aware of a student expressing self-harm or suicidal thoughts must immediately notify the **Director of Guidance**.
- **Parental/Guardian Contact:** The Director of Guidance or designated school administrator will contact the student's parents or legal guardians as soon as possible to inform them of the concern and coordinate next steps.
- **Support & Partner Referral:**
 - School counselors will conduct an initial risk assessment and provide immediate, school-based crisis stabilization.
 - For enhanced assessment, long-term support, or community resources, the school actively partners with **Pickens Behavioral Health**.

Note: A student exhibiting active suicidal ideation or self-harm concerns must not be left unattended at any time during this process. All staff have completed the Jason Flat Suicide Prevention Modules as part of certification.

2. Seizure Safe Schools Procedures

Purpose: In accordance with the **South Carolina Seizure Safe Schools Act (Act 128, 2024; effective July 1, 2025)**, Summit Academy ensures that all staff are prepared to recognize, respond to, and support students with seizure disorders, whether in a **virtual setting** or during **in-person events** (e.g., testing, leadership activities, or field trips).

Seizure Action Plans (SAPs)

- A **Seizure Action Plan (SAP)** shall be developed for any student diagnosed with a seizure disorder.
- The SAP will:
 - Be provided annually by the parent/guardian and signed by the child's licensed healthcare provider.
 - Supplement the student's Individual Health Care Plan (IHP) or 504 Plan, as applicable.
 - Outline emergency procedures, prescribed medication, and individualized supports.
- Copies of SAPs will be stored securely in the **student's digital record** and shared with staff on a **legitimate need-to-know basis**.

Staff Training

- All school staff will complete **annual seizure recognition and response training** consistent with guidelines established by a qualified nonprofit supporting individuals with epilepsy.
- Training will include:
 - Recognizing common signs and symptoms of seizures.
 - Appropriate immediate response steps.

- Administration of seizure medications, if applicable.
- Virtual adaptations (e.g., identifying seizure signs over video calls and initiating emergency response).
- Completion of training will be documented annually.

Emergency Response

- **Virtual Setting:** If a seizure occurs while a student is in a live class session:
 - The teacher will immediately call **911** using the student's registered physical address.
 - The parent/guardian will be contacted without delay.
 - Staff will follow the student's SAP.
- **In-Person Setting:** At testing centers, field trips, or events:
 - A trained staff member will carry copies of SAPs and emergency contact information.
 - Staff will follow SAP protocols, administer prescribed rescue medication (if authorized), and call **911**.

Parent & Guardian Role

- Parents/guardians must provide:
 - Written authorization for seizure medications and action steps.
 - Up-to-date SAP each year.
 - Emergency contact information and consent to share relevant details with staff.

Liability & Indemnity

- As required by law, Summit Academy and its employees shall not be held liable for injuries resulting from following a student's SAP, and parents/guardians must acknowledge this responsibility in writing.

3. Mental Health Services Following Emergencies

Tiered mental health resources are deployed to support students, staff, and families in recovery:

- **Internal School-Based Supports:**
 - **Administration** coordinates crisis response operations, clear communication, and safe spaces on campus.
 - **Director of Guidance** and school counseling staff lead individual/group support sessions
- **External Community Partnership**
 - In events requiring extended care, specialized trauma response, or long-term therapy, the school mobilizes its partnership with **Pickens Behavioral Health** to deploy additional clinicians and triage ongoing mental health needs.

R – OFF CAMPUS EMERGENCY - PRE-PLANNING

Definition: Emergencies that take place off school grounds while students are on a school sponsored activity.

Pre-Trip Planning for all off-campus activities:

Pre-planning is an essential element of trip preparation. The following steps must be completed prior to the off-campus trip:

- 1) Field Trip Request Form completed and approved.
- 2) A roster containing the names of all personnel (students and others) who will be participating in the field trip will be completed in duplicate. One copy of the roster will be maintained at the school and the other given to the driver prior to departure. The school copy will be kept for one year.
- 3) Emergency medical information for each student shall be carried on each field trip.
- 4) All personnel (students and others) riding buses on field trips must have proper identification with them. Note: It is recommended that all students wear armbands on field trips.
- 5) Chaperones are responsible for notifying the school of any delays or changes in the itinerary.
- 6) The school's emergency procedure guide must be carried on all field trips by the chaperones.

Note: These rules apply to all facets of transportation of students. These rules must be part of any contract with any common carrier for the transportation of students. School chaperones are requested to carry cellular phones on all out of district trips.

OFF-CAMPUS EMERGENCY - ACTION STEPS (Levels I, II, or III) Includes personal injury or illness, automobile or bus accident.

Definition: Emergencies that take place off school grounds while students are on a school sponsored activity.

Action Steps:

In the event of an off-campus emergency, school personnel will take the following steps:

- 1) Assist in identifying students who require first aid.
- 2) Contact Emergency Services by calling 911
- 3) Notify the District's Director of Special Services

S – MEDIA PLAN

PHILOSOPHY

The District and School provides access to all public information through cooperative efforts among representatives of the media and district personnel while considering the responsibilities of both parties. The primary objective is to inform the public of all relevant information during a district/school emergency.

REGULATIONS

- 1) The School's Public Information Officer will be the designated person to work with the media. All media requests will be directed through him/her. The School's Public Information Officer will serve as the spokesperson for the School.
- 2) The school office and law enforcement will assign a location for the media which is convenient for them and which will meet the requirements of both the media and school personnel.
- 3) The School's Public Information Officer will provide the media guidelines established by the school.
- 4) The School's Public Information Officer will prepare notes for speakers involved in news conferences and will prepare written statements for the press.
- 5) At no time will students be interviewed without parental approval. When requests for student interviews are granted, the interview will be completed with minimum loss of instructional time, minimum interruption in the learning environment, and approval from the School Leader.
- 6) School personnel will refer all media questions to the School's Public Information Officer.

MEDIA CONTACTS

The School will maintain a list of all local newspapers, radio stations, and television stations. This list will contain the names of contact persons, telephone numbers, and (where available) FAX numbers. When an emergency occurs, these contacts will be notified and plans will begin to accommodate their need to gather information about the emergency.

MEDIA EMERGENCY KIT

- A) Copy of School Emergency Plan
- B) Lists of all media contacts
- C) Name tags for media personnel
- D) Copy of Freedom of Information regulations
- E) Portable computer
- F) Local phone book

T – EMERGENCY EVACUATION PROCEDURES

This guide should be kept with class rosters and used as indicated during any evacuation. As it is not possible to cover every contingency, good judgment and common sense should ensure the effective management of emergency evacuations.

EMERGENCY PHONE NUMBERS

FIRE / POLICE/ EMS: 911 **DISTRICT OFFICE:** 803-734-8322

Director of Special Services: 803-734-8067 (o) 803-230-9593 (c)

SCHOOL CODES:

WHITE:	Medical Emergency
BLUE:	Intruder in building
RED:	Bomb, Explosion, or threat
ORANGE:	Chemical spill or Chemical Emergency
GRAY:	Weather Warning EXTREME WEATHER
BLACK:	Extreme Weather <u>ALERT</u> Directions to follow

ALARMS

FIRE: Fire alarm will sound- STOP — LOOK and LISTEN for announcement. Exit quickly and orderly to the assigned evacuation site. Shut doors as you leave. Take roll and hold up the appropriate color card.

CODE RED: Evacuate building to assigned evacuation site. Take book bags and purses. Do not use walkie-talkies or cell phones in the immediate vicinity of a suspected device. Check evacuation site for secondary devices, face students away from the building, be prepared to drop and cover in the event of an explosion, take roll and hold up appropriate color cards. Do not return until all clear is given.

CODE BLUE: Lock all doors and remain in the room until all clear is given.

CODE WHITE: Announce: “ERT please report to _____.”

CODE GREY: Listen for announcement and follow instructions.

CODE BLACK: Students will assume DUCK AND COVER POSITIONS. Listen for further instructions.

CODE ORANGE: Listen for announcement.

UTILITY SHUT OFF

If utilities need to be shut off, that can be completed at the closet in the teacher’s lounge on the YLA campus. The lounge is located inside building L. To turn off buildings 1-5, the breaker is located behind classroom H. To turn off 8th grade classrooms, the breaker is to the left of classroom B.

FIRST AID AND EMERGENCY SUPPLY LOCATIONS

First aid kits and emergency supplies are located in the Summit Academy, Tall Pines, and Youth Leadership Academy offices. Additionally, designated staff will have first aid kits at in-person events.

U – STUDENT/PARENT REUNIFICATION PROCEDURES

Purpose

Summit Academy recognizes that, while students are primarily served virtually, reunification is critical for **in-person emergencies** (testing sessions, events, or field trips).

Procedures

In-Person Experiences:

- A **designated reunification site** will be established at each event location.
- Parents/guardians must present identification before a student is released.
- Staff will maintain documentation of student release, ensuring each child is reunited only with an authorized guardian.

V – ACCESSIBILITY AND SPECIAL NEEDS ACCOMMODATIONS

Purpose

Summit Academy ensures that all students, including those with disabilities or medical needs, are supported in emergency planning.

Virtual Supports

- Closed captioning, screen-reader-ready documents, and text-to-speech tools will be provided during drills and emergencies.
- Students requiring individualized assistance (e.g., health accommodations, visual impairments) will have these supports noted in their IEP/504/IHP.

In-Person Supports

- Event staff will ensure accommodations for mobility, sensory, and medical needs during evacuations and reunifications.
- SAPs and IHPs will accompany students to in-person events.

W – SAFETY COMPLIANCE FOR PARTNER FACILITIES

Summit Academy does not operate daily student-occupied buildings. However:

- **Administrative offices** comply with local fire and safety codes.

- **Partner facilities** (e.g., testing centers, leadership camps, field trip sites) must maintain compliance with **SC Fire Marshal and Department of Education safety standards**.
- Summit will document **agreements** with facilities confirming they conduct routine inspections of:
 - Fire alarms and sprinklers
 - Kitchen hoods and sanitation systems (if applicable)

X – ROUTINE SAFETY INSPECTIONS & ANNUAL TRAINING

- Summit will conduct **annual reviews** of its crisis and safety plan, training staff on all updates.
- Documentation will include:
 - Annual seizure training (per Act 128).
 - Drill records for both virtual and in-person scenarios.
 - Verification of safety compliance at partner facilities.
- The **first emergency evacuation drill** for in-person events will occur within 10 days of the start of the first scheduled session each year.

Y – SCHOOL OPERATIONS

- **Visitor Management Procedures**
 - Due to the nature of the virtual school, visitors are utilized for in-person events only.
 - All chaperones for in-person events have completed a SLED background check and have completed volunteer training. Records for both are kept on file in the school office.
- **Student Supervision Procedures**
 - Due to the nature of the virtual school, student supervision primarily occurs at home and is supervised by parents. During LIVE lessons, students are expected to have their cameras on, and teachers are able to see students on the screen. If at any time a teacher sees or hears an emergency situation occur, emergency procedures will be followed. At in-person events, staff is in close proximity to all students. No students are left alone in any area. Staff members supervise bathroom areas and all activities.
- **Cybersecurity Incident Response Procedures**

1. Purpose, Scope, and Authority

1.1 Purpose

This document establishes mandatory procedures for detecting, containing, eradicating, and recovering from cybersecurity incidents affecting Summit Academy, and for meeting the school's legal, contractual, and community notification obligations arising from those incidents.

1.2 Scope

This procedure applies to:

- All school-owned or school-managed devices, networks, servers, cloud tenants, and data systems.
- All staff, faculty, contractors, volunteers, and students who access school systems or data.
- Personally owned devices used to access school email, systems, or student data.

- **Third-party and vendor systems** that store, process, or transmit school data — including student information systems, learning platforms, assessment vendors, transportation, food service, payroll, and benefits providers. See Section 9.

Summit Academy operates and maintains its own information technology infrastructure. Escalation and decision authority under this procedure rest entirely with the roles named in Section 4; no external IT organization holds response authority over school systems.

1.3 Authority

The Incident Lead has authority to activate this procedure and to direct the response. Once activated, the Incident Lead's direction supersedes normal reporting lines for the duration of the incident. The Technical Lead has standing authority to isolate individual endpoints or accounts without prior approval where delay would allow the incident to spread.

2. Definitions

- **Event** — Any observable occurrence in a system or network. Most events are not incidents.
- **Incident** — An event that actually or imminently jeopardizes the confidentiality, integrity, or availability of school systems or data, or that constitutes a violation of school security policy.
- **Breach** — An incident in which personal identifying information or protected student records were, or are reasonably believed to have been, acquired or accessed by an unauthorized person. A breach is a legal determination made with counsel, not a technical one made by IT.
- **Personal Identifying Information (PII)** — As defined by S.C. Code § 39-1-90 and applicable federal law; includes name in combination with Social Security number, driver's license or state ID number, financial account or card number with access code, or other data elements specified by statute.
- **Education Record** — As defined by the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and 34 C.F.R. Part 99.
- **IRT** — Incident Response Team, as constituted in Section 4.
- **Threat Actor** — The individual or group responsible for the incident.
- **Out-of-Band Communication** — Communication over channels that do not depend on school-managed systems. See Section 4.3.

3. Severity Classification and Escalation

Severity determines who is notified, how quickly, and what authority is triggered. The Technical Lead assigns an initial severity at triage; the Incident Lead may raise or lower it at any time. When classification is uncertain, the higher level applies until the facts support downgrading.

Level	Definition and Examples	Notification Required	Notification Deadline
1 — Low	Single-user phishing attempt; isolated malware blocked by endpoint protection; no data loss; no account compromise.	IT Helpdesk logs; Technical Lead reviews.	Logged immediately; Technical Lead review within 1 business day. No IRT activation.
2 — Medium	Compromised staff or student account; localized network or system outage; possible unauthorized access to non-sensitive data; suspicious lateral movement.	Technical Lead, Incident Lead. Legal & Compliance Lead consulted. Insurance carrier placed on notice.	Incident Lead within 1 hour of confirmation. Legal within 4 hours. Carrier within 8 hours.
3 — High	Ransomware or destructive malware; confirmed or suspected exposure of student or staff PII; widespread network compromise; business email compromise involving funds; loss of access to critical instructional or safety systems.	Full IRT activation. Legal & Compliance Lead engages outside counsel. Insurance carrier notified before any outside vendor is retained. Governing board chair informed.	IRT within 30 minutes of confirmation, 24/7. Counsel within 1 hour. Carrier within 2 hours. Board chair within 4 hours.

Escalation is not optional and does not wait for business hours.

A Level 3 incident discovered at 11:00 p.m. on a Saturday is called immediately using the out-of-band contacts in Section 4.3. Staff who escalate an event that turns out to be benign have followed this procedure correctly.

3.1 Automatic Escalation Triggers

Any of the following raises an incident to Level 3 regardless of prior classification:

- A ransom note, extortion message, or threat-actor contact of any kind.
- Evidence that data has been copied or transmitted off the network (exfiltration).
- Compromise of a domain administrator, superintendent, principal, or business office account.
- Loss of access to the student information system, payroll, or any system supporting student safety.
- Any incident that will be visible to families, media, or the public before the school can control the message.

4. Incident Response Team

4.1 Roles

- **Incident Lead** — activates this procedure, holds final decision authority throughout the response, and declares closure.
- **Technical Lead** — directs technical triage, containment, eradication, and recovery; assigns initial severity.
- **Legal & Compliance Lead** — engages counsel, owns all notification determinations, and protects privilege.
- **Communications Officer** — sole authorized spokesperson; drafts all external and internal messaging.
- **Safeguarding Officer** — assesses and responds to student welfare impacts (Section 12.1).
- **Operations Lead** — instructional continuity, facilities, and life-safety system status.
- **Scribe** — maintains the factual Incident Log (Appendix A) and the chain of custody record.

4.2 Assignments and Contacts

Role	Primary Assignment	Primary Contact	Backup Assignment	Backup Contact
Incident Lead	David Yeager	850-525-3614	Jason Eichelberger	[Mobile]
Technical Lead	Andy Norris	864-430-0017	David Yeager	850-525-3614
Legal & Compliance Lead	Jason Eichelberger	803-719-1822	Rick Kelley	864-395-9808
Communications Officer	Stacy Kirkland	803-467-3626	Kristen Hendrick	864-230-1152
Safeguarding Officer	Sandee Blankenship	864-430-5999	Shasta Looper	864-321-3445
Operations Lead	Scott Volheim	706-594-4811	Sandee Blankenship	864-430-5999
Scribe	Leigh Fine	864-508-4266	Ansley Cudd	864-918-7536

External Contacts

Contact	Organization	Number / Reference
FBI — Columbia Field Office	FBI	ic3.gov
SLED	SC Law Enforcement Division	[Number]
Local Law Enforcement	[Agency]	[Number]
Clemson University Learning Institute	CULI Leadership	864-878-1103 / Headquarters

4.3 Out-of-Band Communications

School email, chat, phones, and file storage must be treated as compromised and monitored by the threat actor until the Technical Lead confirms otherwise. The IRT does not coordinate the response over school systems during a Level 2 or Level 3 incident.

- **Designated alternate channel:** [e.g., a pre-established encrypted messaging group on personal devices]. Membership is maintained by the Incident Lead and tested at each tabletop exercise.
- **Personal mobile numbers** for every IRT member are held on the printed contact card issued to each member.
- **Personal email addresses** for every IRT member are recorded on the same card as a secondary fallback.
- **Printed copies** of this procedure and the contact card are held by each IRT member at [home / office location] and reissued whenever this document is revised.

Do not discuss the incident on school systems.

Assume the threat actor reads school email and chat. Speculation about cause, blame, scope, or payment written into a school system during an active incident is visible to the attacker and discoverable in later litigation.

5. Phase 1 — Preparation (Ongoing)

5.1 Backups

- Automated backups run daily for all critical systems and student data.

5.2 System Readiness

- The Technical Lead maintains a current inventory of systems, data locations, and the sensitivity of data held in each.
- **Life-safety dependency map:** the Technical Lead and Operations Lead jointly maintain a list identifying which safety systems — door access control, intercom and PA, telephony, emergency notification, fire and alarm panels, camera systems, HVAC controls — depend on the network. This map is consulted before any network-wide disconnection. See Section 7.2.
- Multi-factor authentication is enforced on all sensitive accounts, all remote access, and all administrative accounts.
- Logging is enabled and retained for a minimum of [30] days on endpoints, servers, firewalls, and cloud tenants.

5.3 Training and Exercises

- All staff and faculty complete cybersecurity awareness training annually, with a phishing simulation.
- The IRT conducts at least one tabletop exercise per school year. At least one exercise every two years assumes school email and phones are unavailable and is conducted entirely over out-of-band channels.

6. Phase 2 — Detection, Reporting, and Triage

6.1 Staff Reporting Duty

Any staff member, contractor, or student who observes an anomaly reports it to the IT Helpdesk immediately. Reportable anomalies include locked or encrypted files, ransom messages, unrecognized login alerts, unexpected password reset notices, unusual account activity, missing or altered data, suspicious email requesting payment or credentials, and any device behaving unexpectedly after clicking a link or opening an attachment.

Report first. Do not investigate, remediate, or delete.

Deleting a suspicious email, wiping a machine, or running your own cleanup destroys the evidence needed to determine what happened and whether notification is legally required. There is no penalty for reporting something that turns out to be harmless. Delay in reporting is itself the harm.

6.2 Triage

1. The Technical Lead investigates the report and determines whether an actual incident has occurred.
2. The Technical Lead assigns an initial severity level under Section 3.
3. The Scribe opens the Incident Log (Appendix A) and records the facts.

4. Notification proceeds on the deadlines in the Section 3 table. The clock starts at confirmation, not at the start of the next business day.

6.3 Incident Log

The Incident Log is a factual record: what was observed, when, by whom, what actions were taken, and when. It records observations and actions only.

Analysis, hypotheses about cause, assessments of fault, and discussion of legal exposure do not belong in the Incident Log. Those are recorded separately under counsel direction as described in Section 10.

7. Phase 3 — Containment and Eradication

7.1 Immediate Containment

- **Isolate affected devices** from the network — disconnect the ethernet cable and disable Wi-Fi.
- **Do not power off affected machines** unless directed by the Technical Lead or forensic team. Powering down destroys memory-resident evidence that may be the only record of how the intrusion occurred.
- **Disable compromised credentials** and force password resets. Where lateral movement is suspected, reset all privileged accounts and revoke active sessions and tokens, not only passwords.
- **Suspend third-party integrations and API tokens** that could carry the compromise into connected systems.
- **Preserve evidence:** photograph or screenshot ransom notes and error messages, and export system, firewall, and cloud audit logs before any remediation begins. Log retention windows expire; capture logs first.

7.2 Authority to Disconnect

The Technical Lead may isolate individual devices, accounts, or segments at any time without prior approval.

Disconnection of the network as a whole during instructional hours requires the approval of the Incident Lead, who consults the Operations Lead and the life-safety dependency map (Section 5.2) before deciding. The decision balances the spread of the incident against the loss of systems that support student safety.

If life-safety systems will be affected, the Operations Lead implements manual fallback procedures — [door monitoring, runner communication, handheld radios, alternate emergency notification] — before the disconnection occurs. Where the incident is actively destroying data and no safe interval exists, the Incident Lead may order immediate disconnection and implement fallbacks concurrently.

7.3 Eradication

- Identify and close the initial access vector before restoring anything. Restoring into an unpatched environment reinfects it.
- Remove malicious files, scheduled tasks, services, and accounts created by the threat actor.
- Search specifically for persistence mechanisms: rogue administrator accounts, modified group policy, unauthorized MFA devices or app passwords, mail forwarding rules, OAuth grants, and VPN or remote access configurations.

- Rotate all credentials, service account passwords, API keys, and certificates that the threat actor could have accessed.
- Where outside forensics are engaged, eradication follows the forensic firm's direction so that evidence is not destroyed prematurely.

Retain no outside vendor before the carrier approves.

Most cyber policies require notice before outside forensics, counsel, or negotiators are engaged, and require the use of panel vendors. Retaining a firm independently — including your existing IT provider acting in a forensic capacity — can result in those costs being denied and, in some policies, coverage for the incident being disputed. Confirm with the carrier first.

8. Phase 4 — Recovery

- **Confirm eradication.** The Technical Lead verifies, with the forensic firm where one is engaged, that threat actor access and persistence have been fully removed before any system returns to service.
- **Rebuild rather than clean** where a system was compromised at the operating system level.
- **Restore from the most recent verifiably clean backup.** Verify data integrity before the system is made available to users. Confirm the backup predates the initial intrusion, which is frequently earlier than the date the incident was detected.
- **Reconnect in phases,** prioritizing life-safety systems, then the student information system, then payroll and business operations, then instructional systems, then general access.
- **Reset credentials at scale** before users return, including any credential that could have been captured during the compromise.
- **Enhanced monitoring:** maintain elevated logging and active monitoring for a minimum of 30 days following recovery from a Level 3 incident, and 14 days following a Level 2. Threat actors commonly return through persistence that survived the initial cleanup.
- **Declaring closure:** the Incident Lead declares the incident closed, with the concurrence of the Technical Lead and the Legal & Compliance Lead. Closure requires that eradication is confirmed, affected systems are restored and stable, the enhanced monitoring period has passed without recurrence, all required notifications have been issued, and the Incident Log is complete.

9. Third-Party and Vendor Incidents

A significant share of school data compromises occur at vendors rather than on school networks. This procedure applies when a vendor holding school data is breached, even though school systems are unaffected.

9.1 On Notice of a Vendor Incident

5. Classify under Section 3 based on the school data involved, not on the vendor's own characterization of severity.
6. The Legal & Compliance Lead retrieves the contract and data privacy agreement and identifies the vendor's notification, cooperation, indemnification, and remediation obligations.

7. The Technical Lead determines what school data the vendor held, for which populations and which school years, and whether the vendor held credentials or integration tokens that reach school systems.
8. Revoke and rotate any school credentials, API keys, SSO connections, or integration tokens issued to the vendor.
9. Request from the vendor, in writing: the categories of data involved, the individuals affected, the date range, the vendor's forensic findings, and the remediation offered.
10. Determine independently, with counsel, whether notification obligations are triggered. Do not rely on the vendor's assessment.

The obligation to notify families is the school's, not the vendor's.

Where a vendor breach exposes student or staff data, the school remains the party that owes notice to affected individuals and regulators. A vendor's decision to delay, minimize, or handle its own notifications does not relieve the school of that duty, and the school's community will hold the school accountable regardless of where the failure occurred.

9.2 Ongoing Vendor Management

- Data privacy agreements require vendors to notify the school within a defined period — [24 to 72 hours] — of discovering an incident affecting school data.
- The Legal & Compliance Lead maintains a current inventory of vendors holding student or staff data, with the categories of data held and the contract's breach notification terms.
- Vendor security posture is reviewed at contract renewal.

10. Ransomware, Extortion, and Evidence Handling

10.1 Ransom Payment Decision

No person is authorized to pay a ransom, negotiate with a threat actor, or contact a threat actor by any means except as set out in this section.

- **Authority.** A ransom payment may be made only with the written approval of the Incident Lead, the governing board chair, outside counsel, and the insurance carrier. This authority cannot be delegated and cannot be exercised under time pressure asserted by the threat actor.
- **Sanctions screening.** Payment to a sanctioned entity or jurisdiction is a violation of federal law enforced by the U.S. Treasury Department's Office of Foreign Assets Control, and exposes the school and its officers to liability regardless of duress. Counsel or a carrier-approved negotiator must complete sanctions screening before any payment is contemplated.
- **Communication with the threat actor** is conducted only by a carrier-approved professional negotiator. No school employee communicates with the threat actor directly, including to ask questions, request more time, or verify claims.
- **Payment does not resolve the incident.** Decryption tools frequently fail or work only partially, exfiltrated data is often published or resold regardless of payment, and payment does not remove the notification obligations in Section 11.

10.2 Evidence Preservation and Chain of Custody

- Affected systems are not wiped, reimaged, or returned to service until the Technical Lead, or the forensic firm where engaged, releases them.
- Forensic images are taken before remediation where the incident may result in litigation, insurance claim, or law enforcement referral.
- The Scribe records for each item of evidence: what it is, when and by whom it was collected, and every subsequent transfer of custody.
- Log exports are captured immediately, before retention windows expire.

10.3 Legal Privilege

In a Level 2 or Level 3 incident, the Legal & Compliance Lead engages counsel at the outset, and the forensic investigation is retained by and reports to counsel rather than directly to the school. This is what preserves the attorney-client privilege and work product protection over the investigation.

Two records are maintained and kept separate:

- **The Incident Log** — factual observations and actions. A business record. Assume it will be produced in litigation or regulatory review.
- **The investigative and analytical record** — cause analysis, assessments of exposure, and remediation deliberations. Prepared at the direction of counsel, marked "Privileged and Confidential — Attorney Work Product — Prepared at the Direction of Counsel," and distributed only as counsel directs.

Speculation about cause, fault, or exposure is not written into email, chat, or the Incident Log at any point.

11. External Notification Obligations

The Legal & Compliance Lead owns all notification determinations and confirms current requirements with counsel. The table below is a planning aid, not a substitute for that determination.

Recipient	Trigger	Timing	Owner
Cyber insurance carrier	Any Level 2 or Level 3 incident; any potential claim.	Level 3: within 2 hours. Level 2: within 8 hours. Always before retaining any outside vendor.	Incident Lead
Outside breach counsel	Any Level 3; any Level 2 with possible data exposure.	Within 1 hour of Level 3 confirmation.	Legal & Compliance Lead
SC residents whose PII was breached (S.C. Code § 39-1-90)	Unauthorized acquisition of unencrypted personal identifying information that compromises security, confidentiality, or integrity.	In the most expedient time possible and without unreasonable delay, subject to law enforcement delay requests and the needs of system restoration.	Legal & Compliance Lead
SC Dept. of Consumer Affairs, Consumer Protection Division, and consumer reporting agencies	Breach requiring notice to more than 1,000 SC residents.	Without unreasonable delay, concurrent with individual notice.	Legal & Compliance Lead
Parents and guardians / affected staff	Student or staff data exposure; disruption to instruction, safety, or operations.	As soon as accurate information is available; do not wait for full forensic closure to acknowledge the incident.	Communications Officer
Law enforcement — local, SLED, FBI / IC3	Extortion or ransomware, financial crime or fraudulent transfer, threat to student safety, or suspected criminal intrusion.	Level 3: same day. Coordinate timing with counsel and carrier.	Incident Lead
School authorizer / sponsor and CULI leadership	Any Level 3; any incident affecting student records, instructional continuity, or public reputation.	Within 4 hours of Level 3 confirmation.	Incident Lead
SC Department of Education	As required by applicable reporting requirements and the school's charter agreement.	As specified by the applicable requirement.	Legal & Compliance Lead
IRS (dataloss@irs.gov)	Compromise of W-2 or payroll tax data, including W-2 phishing.	Immediately upon confirmation.	Legal & Compliance Lead
Financial institutions	Fraudulent transfer, compromised banking credentials, or business email compromise affecting payments.	Immediately — recovery of transferred funds depends on speed.	Incident Lead
MS-ISAC / K12 SIX	Any Level 3, for threat	As soon as practical after	Technical Lead

Recipient	Trigger	Timing	Owner
	intelligence sharing and no-cost response support.	containment begins.	

11.1 FERPA Considerations

FERPA does not impose a breach notification requirement of its own, but where a breach results in unauthorized disclosure of education records, the school records that disclosure consistent with 34 C.F.R. § 99.32 and evaluates whether its practices met the standard of reasonable methods for protecting those records. The U.S. Department of Education's Privacy Technical Assistance Center recommends notifying affected families whether or not state law compels it.

11.2 Notification Content

Individual notices are drafted by the Communications Officer, reviewed by counsel before release, and state what happened, what data was involved, when it occurred, what the school has done, what the recipient should do, what remediation is offered — [credit monitoring, identity protection] — and who to contact with questions.

12. Communications Protocol

- **Single spokesperson.** The Communications Officer is the only person authorized to speak about the incident to media, families, or the public. All inquiries are directed there without comment. This instruction is issued to all staff at the moment of IRT activation.
- **Counsel review.** All external communications are reviewed by counsel before release.
- **Holding statement.** A pre-drafted holding statement is maintained in Appendix C and can be released within one hour of a Level 3 activation to acknowledge the incident without speculating.
- **Staff communication.** Staff receive an internal update before external communication goes out where practical, including clear direction on what they may and may not say.
- **No speculation.** Communications state what is known and what is not yet known. Statements about cause, scope, or blame before the investigation is complete frequently prove wrong and become the story.
- **Channel selection.** Where school email and website may be compromised or unavailable, communication uses [SMS notification system, social media accounts, local media, physical notices at school entrances].

12.1 Student Welfare

The Safeguarding Officer assesses student welfare impact in every Level 2 and Level 3 incident and reports to the Incident Lead, addressing:

- Whether student safety information — addresses, custody arrangements, protective orders, safety plans, immigration or health information — was exposed, and whether any individual family requires expedited direct contact.
- Whether any student is placed at heightened risk by the exposure, and what protective steps are required.
- Whether loss of network-dependent safety systems creates a supervision gap requiring adjusted staffing.

- Whether counseling or support should be made available to students or staff.
- Whether mandatory reporting obligations are triggered by anything discovered during the investigation.

13. Phase 5 — Post-Incident Review

- The Incident Lead convenes a lessons-learned meeting with the full IRT within 10 business days of incident closure.
- Where the incident may generate litigation, regulatory review, or an insurance dispute, the review is conducted under counsel direction and its analytical output is treated as privileged under Section 10.3.
- The review addresses: how the incident began, how quickly it was detected, whether escalation occurred on the required timeline, what worked, where the response stalled, and whether the assumptions in this procedure held.
- Every corrective action is recorded with a named owner and a due date. Actions without an owner are not corrective actions.
- The Technical Lead reports completion of technical remediations to the Incident Lead.
- This procedure is updated to reflect what was learned, the version number is incremented, printed copies and offline copies are reissued, and the revision is reported to the governing board.
- The Incident Lead reports the incident and its resolution to the governing board at the next regular meeting, in a format determined with counsel.

14. Document Control

- This procedure is reviewed at least annually by the Incident Lead and Technical Lead, and after every Level 2 or Level 3 incident.
- Contact information in Section 4 is verified at least annually and whenever an IRT member changes.
- Each revision is recorded in the version block on page 1.
- Distribution is restricted. This document describes the school's security posture and response capability and is not posted publicly. Requests for this document under public records law are referred to counsel.
- Superseded printed copies are collected and destroyed when a revision is issued.

Incident Log

Factual record only. Observations and actions. No analysis, speculation, or assessment of fault — those belong in the counsel-directed record described in Section 10.3.

Field	Entry
Incident reference number	
Date and time of discovery	
Discovered by / reported by	
Date and time of first report to IT	
Initial symptoms observed	
Affected systems, applications, accounts	
Data categories potentially involved	
Initial severity and who assigned it	
Severity changes, with time and reason	
IRT members notified, with time of each	
Carrier notified — time, by whom, claim number	
Counsel engaged — time, firm	
Containment actions, with time of each	
Evidence collected and custody transfers	
Notifications issued, with date and recipient	
Recovery actions, with time of each	
Enhanced monitoring period start and end	
Closure declared — date, time, by whom	
Scribe	

Staff Quick Reference

Post at every workstation area and distribute at annual training.

If you see something wrong

11. Stop using the device. Do not click anything further.
12. Do not delete anything, do not run cleanup tools, do not turn the machine off.
13. Disconnect it from the network — unplug the ethernet cable and turn off Wi-Fi — if you can do so without powering down.
14. Call the IT Helpdesk at [number] immediately. Call; do not email, in case email is affected.
15. If you cannot reach the Helpdesk, call [Technical Lead] at [mobile].
16. Write down what you saw and what time you saw it.
17. Do not discuss the incident with anyone outside the school. Refer all questions to [Communications Officer].

Report it even if you think you caused it.

The response depends on knowing quickly. Clicking a bad link is not a disciplinary matter; concealing it while the intrusion spreads is a far more serious problem for everyone.

Signs worth reporting

- Files that will not open, are renamed, or have unfamiliar extensions
- A ransom message or any demand for payment
- Login alerts, MFA prompts, or password reset notices you did not initiate
- Email in your sent folder that you did not send
- A colleague or vendor asking you to change payment details or send funds urgently
- A device that slowed dramatically or behaved oddly after you opened an attachment or link
- Anything that seems wrong and you cannot explain

Holding Statement Template

For release within one hour of a Level 3 activation, after review by counsel. Acknowledges the incident without speculating.

Summit Academy is currently responding to a cybersecurity incident affecting some of our information systems. We identified the issue on August 12, 2026 and immediately began our response, which includes engaging outside cybersecurity specialists and notifying appropriate authorities.

[Statement of operational status — whether school is in session, which services are affected, what families should expect today.]

We are working to determine the full scope of the incident, including whether any personal information was affected. That review takes time, and we are not going to speculate ahead of the facts. If we determine that personal information was involved, we will notify those affected directly and provide information about steps they can take.

We will provide updates at [channel] as more information becomes available. Questions may be directed to [contact].

We appreciate the patience of our families and staff while we work through this.

What the holding statement does not do

- Name a cause, a threat actor, or a suspected entry point
- Estimate how many people are affected
- Promise a restoration date
- State that no data was accessed before the investigation supports that conclusion
- Assign blame to a vendor, an employee, or anyone else
-

Field	Value
Document Version	3.0
Supersedes	Version 2.0, August 12, 2026
Last Updated	August 12, 2026
Approved By	David Yeager – Director of IT
Owner	Director of IT
Next Scheduled Review	08/01/2027
Classification	Internal — Restricted Distribution

•

Offline copy required.

A ransomware event may encrypt the very systems that store this document. Printed copies must be held by every Incident Response Team member at the locations listed in Section 4, and a copy must be stored on offline media in the location designated in Section 5.1.

Not legal advice.

The statutory references in Section 11 are provided as planning aids. Notification obligations change and depend on the facts of the incident. Legal counsel confirms all applicable deadlines and recipients at the time of the incident.

Z – COMMUNICATION PROCEDURES

- **Procedures for staff**
 - The Guard 911 mobile app will be utilized for all staff communication in the event of a campus emergency or crisis. This app notifies staff members through an alert. GroupMe messaging will be utilized when appropriate.
- **Procedures for students**
 - Communication to students in the event of an emergency will be through staff members. Staff members will be alerted by the principal or director.
- **Procedures for parents/guardians**
 - Bright Arrow will be utilized to communicate to parents in the event of an emergency. This PowerSchool plug-in will send text messages and emails with information.
- **Procedures for emergency responders**
 - The Guard 911 mobile app will be utilized during an emergency. This app alerts local law enforcement, as well as law enforcement in the area, by providing an alert. Additionally, the campus SRO will be our liaison with local law enforcement.
- **Procedures for the Authorizer**
 - The director of schools will communicate the emergency to the South Carolina Public Charter School District.
- **Procedures for the Governing Board**
 - The director of schools will communicate the emergency information to our governing board.
- **Procedures for the media**
 - Communication with the media will be conducted by the director of schools or principal following media guidelines in Section S.

AA– YOUTH LEADERSHIP ACADEMY (YLA)/ CLEMSON UNIVERSITY LEARNING INSTITUTE (CULI)



BB – TALL PINES STEM ACADEMY (TPSA)/ CAMP LONG SITE MAP

CAMP LONG



82 Camp Long Road, Aiken, SC 29805



- | | |
|---|---|
| A Administration Building | M White Oak Cabin |
| B The Barn | N Vesper Ring |
| C Kickball Field | O Outdoor Classroom/
Fishing Pier |
| D Gym | P Thompson Hall |
| E Low Ropes Teams Course | Q Morris Lodge |
| F High Adventure Tower | R Dogwood Cabin |
| G Outdoor Courts
Basketball, Volleyball, & Gaga | S Med Shed/ Wash House |
| H The Ark | T Azalea Cabin |
| I Longleaf Leadership Center | U Recreation Field |
| J Dining Hall | V Waterfront |
| K Loblolly Cabin | W Lower Recreation Field |
| L Knotty Pine Cabin | P Parking |

TALL PINES STEM ACADEMY

- 1 Main Office
- 2 Multipurpose Building
- 3 7th Grade Classroom
- 4 7th Grade Classroom
- 5 7th Grade Classroom
& Leadership (all grades)
- 6 8th Grade Classroom
- 7 8th Grade Classroom
- 8 8th Grade Classroom
- 9 8th Grade Classroom
- 10 5th Grade Classroom
- 11 5th Grade Classroom
& Special Ed (all grades)
- 12 6th Grade Classroom
& Special Ed (all grades)
- 13 6th Grade Classroom
- 14 6th Grade Classroom
- 15 Timberwolf Commons
- P Parking