Below is a draft procedure for responding to **anonymous or digital threats** targeting Ridley.

**Policy Name:** Anonymous or Digital Threat Procedure  
**Effective:** [Insert Date]  
**Next Review:** [Insert Date]  
**Responsibility:** Responsible Department: Campus Security, IT Services, Administration

**Procedure Contact:** Manager of Campus Safety and Security

**Approval:** Director of Facilities and Executive Leadership Team

**Purpose**  
This procedure provides direction for responding to anonymous or digital threats made against the school to ensure the safety and security of students, faculty, staff, and visitors while minimizing disruption to school operations.

**Procedure Statement**  
This procedure was developed to address threats made by anonymous or digital means, such as through email, social media, or phone calls, and to outline a systematic response framework that prioritizes safety and communication.

**Scope**  
This procedure applies to any situation where the school is targeted by a threat communicated through anonymous or digital channels. It covers initial actions, threat assessment, communication, and escalation protocols.

**Emergency Response Definitions**

* **LEVEL 1 - General Awareness:** A vague or non-specific threat where the credibility or severity is low but precautionary measures are required. Normal operations may continue while heightened awareness is maintained.
* **LEVEL 2 - Moderate Threat:** A specific, credible threat requiring precautionary actions, such as securing the campus, implementing a hold-and-secure, or contacting law enforcement for support.
* **LEVEL 3 - Severe Threat:** A highly credible or imminent threat requiring immediate lockdown or evacuation of the campus, initiated under law enforcement guidance.

**Emergency Notification Procedure**

1. **Report:** Any staff member who receives or becomes aware of a threat must immediately notify Campus Security and the Manager of Campus Safety.
2. **Assess:** Campus Security will assess the threat's credibility with input from law enforcement and IT Services (for digital threats).
3. **Activate Response:** Based on the assessment, the Manager of Campus Safety will implement the appropriate response level and notify the Executive Leadership Team.
4. **Communicate:** Approved notifications will be sent to staff, students, and parents through the school’s communication system.

[Add communications flow and approvals hierarchy]

**Responsibilities**

**Campus Security Team**

* Record all threat details, including time, nature, and origin.
* Conduct an initial assessment of the threat's credibility.
* Notify law enforcement for further investigation and guidance.
* Assist with implementing the appropriate safety response (e.g., hold-and-secure or lockdown).

**IT Services**

* Analyze the source of digital threats using available technical tools.
* Preserve digital evidence (e.g., emails, social media posts, logs) for investigation.
* Collaborate with law enforcement to track and trace the origin of the threat.

**Manager of Campus Safety and Security**

* Coordinate with law enforcement to evaluate and manage the threat.
* Determine the appropriate response level and implement it.
* Communicate with the Headmaster and Executive Leadership Team regarding updates and decisions.
* Ensure all staff are informed and that students are accounted for during the response.

**Executive Leadership Team (ELT)**

* Provide leadership support and guidance during the response.
* Engage with external stakeholders, such as parents and media, if required.
* Evaluate and debrief after the incident to refine future responses.

**Staff**

* Remain calm and follow instructions issued by Campus Security or the ELT.
* Keep students in secure areas as directed.
* Report any additional suspicious activities or communications.

**Students**

* Follow instructions from staff and security personnel.
* Stay calm and remain in designated safe locations until further notice.
* If students become aware of a threat to the school, they should be guided to inform staff immediately and to retain messages if possible.

**Supplementary Duties**

* **LEVEL 1 Response:**
  + Heightened monitoring of digital communications.
  + Disseminate general awareness updates to staff and security.
* **LEVEL 2 Response:**
  + Lock exterior doors and restrict campus access (hold-and-secure).
  + Work closely with law enforcement to investigate and mitigate the threat.
* **LEVEL 3 Response:**
  + Initiate lockdown and secure all individuals on campus.
  + Provide law enforcement with access to surveillance systems and communication logs.

**Approval Dates:**

* Initial Approval: [Insert Date]
* Revisions: [Insert Date]