**Threats**

Viruses – These low-cost laptops may not come with the necessary protection to guard against viruses that maybe be contracted from the internet of passed around in the P2P networks.

Sub-policies:   
Anti-Virus Policy  
Internet Use Policy  
Disaster Recovery Policy

Unauthorized access to P2P system: Attackers generally will have little problems connecting to an ad-hoc device if they get within signal range allowing them un authorized access to the network.

Sub-policies:  
Remote Access Policy  
Password Policy  
Disaster Recovery Policy

Physical hard: Because these are being widely distributed to a large number of young children there is a very high chance a large number of the laptops will sustain physical damage at school or home.

Sub-policies:  
Disaster Recovery Policy  
Password Policy  
Email Policy

**Purpose**

The purpose of this policy is to create standards for the us of the laptops to be distributed to first form secondary students. This is to ensure the security of the data of on the multiple laptops and to maximize the life of each student’s laptop.

**Scope**

This policy will encompass all the distributed laptops to all form one students and the P2P networks that are created with these laptops.

Ownership and Responsibilities:

All P2P networks that are created for the sharing of data and laptops fall under the responsibility of the respective school’s IT technician.

**Policy**

- Networks must be over seen by school’s IT technician or teacher.

- Monthly check on laptops must be done

- Checks on software must be done monthly

- Administrative actions should only be able to be done through the login of a registered admin which may be the school’s IT technician or a representative from the government

- VPN should be used when logging into internal network