RANSOMWARE PROCEDURE

If you suspect there is ransomware on the school network follow these steps immediately

ISOLATION – BRING WHOLE NETWORK DOWN TO PREVENT IT SPREADING.
STEP 1 - Pull the power leads to all the switches in the server room.

STEP 2 - Disconnect *Backup Servers* from the network (*Location*) *If not already done*

STEP 3 - Disconnect Ethernet cables from back of each server and shutdown servers not in use in the following order.

- *Servernames*
- *Wireless controller*

STEP 4 - Inform *SLT Names Here* of what is happening.

IDENTIFY SOURCE AND ISOLATE
STEP 5 - On an affected server, perform a search for the ransom note filename. The exact filename will vary depending on the malware variant.

STEP 6 - Once the search is complete, add a column to the Windows Explorer list for owner. Or find a file Right click -> Security -> Advanced -> Owner.

This enables you to quickly see which user created all of the ransom notes. You should also be able to see the timestamps for creation as well. If all the owners appear to be the same, it is likely that only a single machine was compromised.

STEP 7 - Isolate the workstation / workstations for this user / users.
Use impero to find the computer used and disconnect from the network immediately. Deactivate users AD account and machine in AD.

DAMAGE REPORT
STEP 8 – Use included report to run through servers running a full virus scan and search for ransom notes based on what was found in Step 5.

STEP 9 - Assess quality of backups and ensure infection hasn't spread to these servers. (*Backup Servers Names*)

INFORMATION GATHERING & CLEANING
STEP 10 – Clean the infected computers. If the Endpoint's AV is up to date, a full system scan should be run to find any copies of the malware to find which malware it was.

STEP 11 - Format HDD on affected computers.

STEP 12 – If ransomware infection has been cleaned and only some files were affected and have been removed power on the switches and start network back up with priority given to the admin network.

STEP 13 – Monitor admin network to ensure no more encryptions take place.

STEP 14 – Bring the curriculum network back online.

- Start the three servers.
- Bring computers back online block by block.
- Monitor network for any further encryptions.

STEP 15 – Restore the affected users files from a good backup.

STEP 16 – If encryption has spread across large parts of the network (Whole G drive or other shares) restores will need to be carried out from most recent backups taken.

STEP 17 – Bring wireless network back online.

STEP 18 - Speak with the user identified in Step 6 to try and identify the file or email that started the infection. Has this file been stored anywhere where it can be relaunched - or has the email been forwarded on to anyone? Depending on the variant it may have been a file on a USB stick, or an attachment, or even a website visited. Try to determine the initial cause and delete where appropriate. You can scan suspicious files and URLs using https://www.virustotal.com.

INFECTION SOURCES

INFECTION SOURCE USER / COMPUTER	TIME	HOW? Email, website, usb?	NOTES

SERVER CHECKLIST

PRIORITY	SERVER NAME	RANSOM NOTES FOUND	AV REPORTED AS CLEAN	NOTES
1				
2				
3				
4				
5				
6				

7				
8				