1. Do/did the hard disks contain(ed) data that is/was protectively marked or classified as OFFICIAL, SECRET or TOP SECRET?
   The hard disks will be blank with no data.

2. Are/were the hard disks encrypted, and if so, to what standard of compliance?
   The hard disks are no longer encrypted.

3. Were the laptop hard disks removed and destroyed, and if so, to what standard of compliance? *(If the hard disks remain in the laptops then...)*
   The hard disks have not been removed.

4. Is a user required to enter a 'BIOS password' or similar pre-boot credentials before any of the laptops boot into the operating system stored on the hard disk?
   No requirement for a BIOS password.

5. Have any accounts and cached credentials on the laptops been secured against brute force attack and other kinds of attack, and if so, how?
   The laptops have no accounts as they have been wiped to NCSC standards.

6. Have any laptop network connections been secured against unauthorised connectivity or attack, and if so, how?
   Not applicable as no operating system installed.

7. Have any physical laptop connections and ports such as USB ports been secured against unauthorised attack, and if so, how?
   Not applicable as no operating system installed.

8. Have school IT administrators been issued with instructions as to how to repurpose the laptops securely, and if so, please can we see these instructions?
   No advice has been given to the school.