RAK AA
RAS AL KHAIMAH AMERICAN ACADEMY
أكاديمية رأس الخيمة الأمريكية

Policy for Use of Removable Media, Such as USB "Thumb" Drives

There is a wide increase in the number of IT security threats originating from removable media which infect systems with malicious code and/or remove sensitive data.

Removable media typically consists of portable devices that can be used to copy, save, store and/or move data from one system to another. Media devices come in various forms that include, but are not limited to, USB drives, flash drives or cards, read/write CDs, memory cards, external hard drives and Personal Digital Assistant (PDA) storage cards.

While removable media are extensively used for storing and transporting data, some of the characteristics that make them convenient to use also introduce security risks, due in large part to the fact that they are typically unmanaged storage devices.

The IT department recommends that all staff and students implement several best practices with regard to removable media devices to assist in mitigating the associated risks.

The following policy is effective immediately based on these best practices:

IT Policy:

- Do not use personally owned removable media devices in school systems.
- Do not use school owned removable media devices on personal machines.
- Do not put unknown removable media devices into ANY system.
- Keep personal systems up-to-date with the latest patches and anti-virus signatures.

Your compliance with this policy and implementation of other mitigating measures is imperative for the protection of RAKAA's information and systems.

We appreciate your diligence on this matter.

IT Department