Bring Your Own Device Policy

Definition of BYOD

For purposes of this policy, BYOD means privately owned wireless and/or portable electronic hand held equipment that includes, but is not limited to, existing and emerging mobile communication systems and smart technologies, portable internet devices, tablets, phones, laptops, hand held entertainment systems or portable information technology systems that can be used for word processing, wireless Internet access, image capture/recording, sound recording and information transmitting/receiving/storing, etc.

School Network

Only the internet gateway provided by the school may be accessed whilst in class. Personal internet connective devices such as, but not limited to mobile phones/ mobile network adapters are not permitted to be used to access outside internet sources during instructional time.

When a student connects their device to the BYOD network for the first time the system puts them on a separate part of the network (VLAN) which is isolated from the main school systems.

When a student first opens a web page the system will send them to a captive portal. They will need to do this each day. This is to stop students from authenticating a device and then someone else using it. At the end of the day the authentication will be lost reducing long term abuse of system.

If students do not enter their school log-on details they will only be allowed access to a filtered list of internet sites e.g. school VLE, school website and GCSE Bitesize.

If students enter their school login details, this will allow them access to an appropriate level of filtering for the internet, allowing the school to track the information and give limited access to other school services

Security and Damages

Responsibility to keep the device secure rests with the individual owner. The school is not liable for any device stolen or damaged whilst at school. If a device is stolen or damaged, it will be handled through the administrative office similar to other personal items that are impacted in similar situations. It is recommended that skins or stickers are used to physically identify devices. Additionally, protective cases for technology are encouraged.

BYOD Student Agreement

The use of technology to provide educational material is not a necessity but a privilege. A student does not have the right to use his or her laptop, mobile phone, tablet or other electronic device while at school. When abused, privileges will be taken away. When respected, they will benefit the learning environment as a whole.

Students and parents/guardians participating in BYOD must adhere to the student Code of Conduct, as well as all related policies, particularly the school's Acceptable Use Policy. In addition:

- Students take full responsibility for his or her device and keeps it with himself or herself at all times. The school is not responsible for the security of the device
- The device must be in silent mode in class when not being used for legitimate educational purposes
- Devices may not be used to cheat on exams, assignments or tests, or for non-instructional purposes (such as making personal phone calls and text/instant messaging) during class
- Devices may not be used to record, transmit or post photographic images or video of a person, or persons during school activities and/or hours.
- Students may access only files on the computer or internet sites which are relevant to the classroom curriculum. Games are not permitted without permission during class time
- Students must comply with teachers' request to turn off any device during class
- Students acknowledge that the school's network filters will be applied to their connection to the internet and will not attempt to bypass them during class

- Students understands that bringing on premises or infecting the network with a virus or other malware designed to damage, alter, destroy, or provide access to unauthorized data or information is in violation of the AUP policy and will result in disciplinary actions
- It is a condition of access that all devices are installed with appropriate anti-virus software which maintained and up to date
- Students realize that processing or accessing information on school property related to "hacking", altering, or bypassing network security policies is in violation of the AUP policy and will result in disciplinary actions
- The school has the right to collect and examine any device that is suspected of causing problems or was the source of an attack or virus infection
- Students understand that access to the internet during class may not automatically allow uploading or downloading of files
- Student realizes that printing from personal devices will not be possible at school
- Students are responsible for ensuring devices are charged prior to bringing them to school. Devices cannot be charged whilst at school

I understand and will abide by the above policy and guidelines. I further understand that any violation may result in the loss of my network and/or device privileges as well as other disciplinary action.

_____ _____

Signature of Student Date

_____ _____

Signature of Parent/Guardian Date