Bring Your Own Device Policy - Students

Author	IT Services
Date	April 2021

Document Control

Version	Date	Change	Change By
V1.0	April 2021	Document creation	Stephane Vernoux
V2	August 2021	Document review following (KCSIE) 2021	Stephane Vernoux

1 Introduction

The Leigh Academies Trust (LAT) recognises the benefits that can be achieved by allowing students to use their own electronic devices when at their academy. Such devices include laptops and tablets, and the practice is commonly known as 'bring your own device' or BYOD. LAT is committed to supporting students in this practice and ensuring that as few technical restrictions as reasonably possible are imposed on accessing LAT provided services on BYOD.

The use of such devices to create and process LAT information and data creates issues that need to be addressed, particularly in the area of information security.

LAT must ensure that it remains in control of the data for which it is responsible, regardless of the ownership of the device used to carry out the processing. It must also protect its intellectual property as well as empowering students to ensure that they protect their own personal information.

2 Principles for Use

- The students are expected to have regard to this policy at all times to protect its electronic communication systems from unauthorised access and harm.
- The objective of this policy is to define the standards of conduct when employing the use of non-school owned electronic devices such as laptops and tablets, used to access the internet and school learning resources.
- The academy reserves the right to refuse to allow access to particular devices or uses where it considers there is a risk to the academy network.
- Use of personal BYOD devices is at the discretion of the academy and should not be seen as a right. Students' own devices can be used in the classroom only at the teacher's discretion.

3 Acceptable Use of User Owned Devices

- The primary purpose of personal devices at school is educational or related to educational experiences. Use of personal devices during the school day is at the discretion of the staff. Pupils must use devices only as directed by their teachers.
- All BYOD devices should only contact the Internet and local area network via the academy wireless network. All internet access via the network is logged.
- The use of cellular data (e.g. GPRS, EDGE, 3G, 4G, etc) to access the Internet in school is strictly prohibited. All access must be by the academy wireless network which is appropriately filtered. It is a condition of BYOD use under this policy that students are responsible for disabling cellular data on their device when on the academy site.
- It is prohibited to use your device to take pictures, video, sound recordings of any student or staff member without their permission.
- It is the students' responsibility to keep their device safe while at school, on school related visits and school sponsored activities.
- The academy does not provide technical support for the students' own devices. Users should be competent in the use of their own device.
- A specific Trust certificate may need to be downloaded before access is granted.
- No linux distributions based devices allowed (Fedora, Ubuntu…).
- No Smart-phone allowed

4 Unacceptable Use of User Owned Devices

- The academy does not approve any 'apps' or updates that may be downloaded onto any device whilst using the academy's wireless network and

such activity is undertaken at the owner's risk. The academy has no liability for any consequent loss of data or damage to the individual's device.

- Devices must not be used in a manner that would portray the academy in an unfavourable light.
- Devices should not be used to intimidate, abuse or share information that might be perceived as unfavourable against any member of staff, student or any person associated with the academy.
- Devices must not be used for accessing, promoting or circulating extremist, racist and homophobic information.
- Devices must not be used to share any information of an indiscrete or sexual nature with any other person.
- Students are not permitted to use any device to create a wireless hotspot.

5 Theft, Damage and Insurance

The academy takes no responsibility for any damage, loss, malware, theft, or insurance of any device that is not the property of the academy, used within the academy premises, including any event which causes the device not to function. We will investigate the theft, but not the loss of a device. If a device is stolen or damaged while on school premises, it is to be reported to student services immediately, in order that the incident can be logged.

It is the students'/parents' responsibility to ensure that they have sufficient personal insurance to adequately cover the device for any such occurrence. Any other costs, including the download of data, incurred while using devices, are not chargeable against the academy and are the sole responsibility of the owner.

6 Monitoring and Access

LAT will constantly monitor the network but will not routinely monitor personal devices. However, it does reserve the right to:

- Prevent access to a particular device from either the wired or wireless networks or both;
- Prevent access to a particular system;
- Take all necessary and appropriate steps to retrieve information owned by LAT.
- Require access to a student's personal device whilst investigating cases of policy breach including, but not limited to, finding or retrieving lost messages lost due to computer failure, to assist in the investigation of wrongful acts including cyber bullying, hacking of the school's computer system, virus attack or to comply with any legal obligation.

7 Data Protection and BYOD

LAT must process 'personal data' i.e. data about identifiable living individuals in accordance with the Data Protection Act 2018. Sensitive personal data is information that relates to race/ethnic origin, political opinions, religious beliefs, trade union membership, health (mental or physical) or details of criminal offences. This category of information should be handled with a higher degree of protection at all times.
LA recognises that there are inherent risks in using personal devices to hold personal data. Therefore, students must follow the guidance in this document when considering using BYOD to process personal data.

For more information see the LAT's Data protection Policy.
.