Bring Your Own Device Policy - Staff

Author	IT Services
Date	September 2018

Document Control

Version	Date	Change	Change By
V1.0	Sep 2018	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 staff to use their own electronic devices when working, whether that is at home, or at their academy or while travelling. Such devices include laptops, smartphones and tablets, and the practice is commonly known as 'bring your own device' or BYOD. LAT is committed to supporting staff 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, therfore we do not allow BYOD for any staff given a device by the Trust.

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 staff to ensure that they protect their own personal information.

2 Information Security Policies

All relevant LAT policies still apply to staff using BYOD. Staff should note, in particular, the LAT's IT Acceptable Use Policy Several of these are directly relevant to staff adopting BYOD.

- Internet Access Policy
- Online Safety Policy
- Data protection Policy

3 The Responsibilities of Staff Members

Individuals who make use of BYOD must take responsibility for their own device and how they use it. They must:

- Connect to a BYOD Wifi network - Not the LAT Wifi network.
- A specific Trust certificate may need to be downloaded before access is granted.
- No linux distributions based devices allowed (Fedora, Ubuntu…)
- Familiarise themselves with their device and its security features so that they can ensure the safety of LAT information (as well as their own information);
- Invoke the relevant security features;
- Maintain the device themselves ensuring it is regularly patched and upgraded;
- Ensure that the device is not used for any purpose that would be at odds with the IT Acceptable Use Policy.

While LAT IT staff will always endeavour to assist colleagues wherever possible, the LAT cannot take responsibility for supporting devices it does not provide.

Staff using BYOD must take all reasonable steps to:

- Prevent theft and loss of data;
- Keep information confidential where appropriate;
- Maintain the integrity of data and information;
- Take responsibility for any software they download onto their device.

Staff using BYOD must:

- Set up passwords, passcodes, passkeys or biometric equivalents. These must be of sufficient length and complexity for the particular type of device;
- Set up remote wipe facilities if available and implement a remote wipe if they lose the device;
- Encrypt documents or devices as necessary;
- Not hold any information that is sensitive, personal, confidential or of commercial value on personally owned devices. Instead they should use their

device to make use of the many services that the LAT offers allowing access to information on LAT services securely over the Internet;
- Where it is essential that information belonging to the LAT is held on a personal device it should be deleted as soon as possible once it is no longer required. This includes information contained within emails;
- Ensure that relevant information is copied back onto LAT systems and manage any potential data integrity issues with existing information;
- Report the loss of any device containing LAT data (including email) to the IT Help desk;
- Be aware of any Data Protection issues and ensure personal data is handled appropriately;
- Report any security breach immediately to IT Helpdesk (the Data Protection Officer will be informed where personal data is involved);
- Ensure that no LAT information is left on any personal device indefinitely. Particular care must be taken if a device is disposed of/sold/transferred to a third party.

4 Monitoring and Access

LAT will not monitor the content of user owned devices, but reserves the right to monitor any traffic over the school system to prevent threats to the school network systems. Also LAT reserves 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.

5 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.

LAT, in line with guidance from the Information Commissioner's Office on BYOD recognises that there are inherent risks in using personal devices to hold personal data. Therefore, staff must follow the guidance in this document when considering using BYOD to process personal data.

A breach of the Data Protection Act can lead to the LAT being fined. Any member of staff found to have deliberately breached the Act may be subject to disciplinary measures, having access to the LAT's facilities being withdrawn, or even a criminal prosecution.

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

.