LIFE ACADEMIES TRUST

LEARN • INNOVATE • FLOURISH • EXCEL

Bring Your Own Device

Document Detail	
Type of Document (Stat Policy/Policy/Procedure)	Policy
Category of Document (Trust HR-Fin-FM-Gen/Academy)	GEN
Index reference number	22
Approved	11/07/2019
Approved by	Trust Board
Next Review date	11/07/2021
Version	V1.2

Date	Version	Revision Description
21/05/18	1	Introduced for GDPR purposes
19/07/18	1.2	Security of Staff Personal Devices updated

Contents

1. Introduction

LIFE Academies Trust recognises the benefits of mobile technology and is committed to supporting staff in the acceptable use of mobile devices.

This policy describes how any electronic device not owned by the Trust (for example laptops, smart phones and tablets) may be used by staff members and visitors to the Trust. This practice is commonly known as 'bring your own device' or BYOD, and these devices are referred to as 'personal devices' in this policy. If you are unsure whether your device is covered by this policy, please check with the Network Manager.

2. Definitions

Any reference to 'Trust' throughout this policy applies to LIFE Academies Trust and the Academies/Settings within it.

3. Organisational Arrangements

Overall Responsibility

The CEO is responsible for the approval of this policy.
Each Academy Principal/Head of setting is responsible for policy implementation and reviewing its effectiveness.

Roles & Responsibilities

Staff members will:

- Familiarise themselves with their device and its security features so that they can ensure the safety of Trust information.
- Install relevant security features and maintain the device appropriately.
- Set up passwords, passcodes, passkeys or biometric equivalents on the device being used.
- Set up remote wipe facilities if available, and implement a remote wipe if they lose the device.
- Encrypt documents or devices as necessary.
- Report the loss of any device containing school information immediately to the relevant Academy Principal/Head of Setting and Network Manager.
- Report any data breach in line with the Data Breach policy.
- Ensure that no school 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.

Visitors will:

- Familiarise themselves with the use of personal devices at the Trust.
- Only use personal devices for agreed purposes at the Trust and with the relevant permission.
- Not share any Trust-related data/information in any way and will not retain any Trust-related data/information after leaving the site.

4. Detailed Arrangements & Procedures

Use of personal devices at the Trust

Staff and visitors to the Trust may use their own devices in the following locations:

- In the classroom, only with the permission of the teacher.
- In the Trust environments e.g. libraries, sports pitches and outdoor spaces.

Personal devices must be switched off when in a prohibited area, and / or at a prohibited time, and must not be taken into controlled assessments and / or examinations unless special circumstances apply.

The Trust reserves the right to refuse staff and visitors permission to use their own device on Trust premises.

Use of cameras and audio recording equipment

Parents and carers may take photographs, videos or audio recordings of their children at Academy/Setting events for their own personal use in line with the Trust *Photography and Use of Images* Policy.

Only official sanctioned visitors authorised by the relevant Academy Principal/ Head of Setting and staff may use their own personal devices to take photographs, video, or audio recordings in Academies/Settings during the school day (see parents separately referred to the Trust *Photography and Use of Images* Policy) having first ensured that parental permission has been received by the Academy/Setting for any photographs taken. This includes people who may be identifiable in the background.

Photographs, video or audio recordings made by staff or authorised visitors on their own devices should be deleted as soon as reasonably possible after they have been used, e.g. uploaded for use on one of the Trust's social media sites. Photographs, video or audio recordings to be retained for further legitimate use, should be stored securely on the Trust network.

Photographs, video or audio recordings should not be published on blogs, social networking sites or in any way without the permission of the people identifiable in them.

Devices must not be used to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely to take photographs, video or audio recordings in Academies/Settings.

Access to the Trusts internet connection

The Trust provides a wireless network that staff and visitors to the Trust sites may use to connect their personal devices to the internet. Access to the wireless network is at the discretion of the relevant Academy/Setting, and access may be withdrawn for anyone considered to be using the network inappropriately.

The Trust cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk. The Trust is not responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the Trust's network. The Trust will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the Trust's network.

Access to Trust systems

Staff are permitted to connect to or access Trust cloud-based services (e.g. E-Mail, Calendars, file storage) from their device.

Staff may use the systems to view Trust information via their personal devices, including information about pupils. Staff must not store the information on their devices, or on cloud servers linked to their device. In some cases, it may be necessary for staff to download school information to their personal devices in order to view it (e.g. an email attachment). Staff shall delete this information from their device as soon as they have finished viewing it.

Staff must only use the IT systems and any information accessed through them for work purposes. Trust information accessed through these services is confidential, in particular information about pupils. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to, or distribution of, confidential information should be reported as per the Data Breach Policy.

Staff must not send Trust information to their personal email accounts.

Monitoring the use of personal devices

The Trust may use technology that detects and monitors the use of personal devices which are connected to the Trust's wireless network or IT systems. By using a device on the Trust's network, staff and visitors agree to such detection and monitoring. The Trust's use of such technology is for the purpose of ensuring the security of its IT systems and tracking Trust information.

The information that the Trust may monitor includes, (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms, information uploaded or downloaded from websites and Trust IT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Staff who receive any inappropriate content through Trust IT services or the Trust internet connection should report this to the Technical Support Department as soon as possible.

Security of staff personal devices

Any member of staff wishing to use their own device must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption. This should be more than a simple password protection.

Staff must ensure that personal devices are set to lock with encrypted passcodes (alphanumeric passwords are potentially stronger than purely numerical passcodes) to prevent unauthorised access. The device should be locked if they are unattended or set to auto-lock if it is inactive for a period of time. Staff using a shared or public computer must always log out when left unattended.

Staff must never attempt to bypass any security controls in school systems or others' own devices.

Staff must ensure that appropriate security software is installed on their personal devices and must keep the software and security settings up-to-date.

Staff must ensure that passwords are kept securely and are not accessible to third parties.

Devices that are jail-broken, rooted or similarly compromised present a significant risk to the security of Trust data and systems and must not be used to access either.

Staff should also make reference to their responsibilities for security listed under point 3 above – roles and responsibilities.

5. Support

The Trust takes no responsibility for supporting staff's own devices, nor does the Trust have a responsibility for conducting annual PAT testing of personal devices. However, the Trust will support staff in ensuring that they have appropriate levels of security in place.

6. Compliance, sanctions and disciplinary matters for staff

Non-compliance of this policy exposes both staff and the Trust to risks. If a breach of this policy occurs, the Trust Disciplinary policy will be applied.

7. Incidents and reporting

The Trust takes any security incident involving a staff member's or visitor's personal device very seriously and will always investigate a reported incident. Loss or theft of the device should be reported to the appropriate school office in the first instance. Data protection incidents should be reported immediately to the relevant Academy Principal/Head of Setting.