Bring Your Own Device Policy

Document Control

Version	Author	Summary of Changes	Approved By	Date Published	Date of Review
1	MPI	New policy	F&O Committee	Feb 2023	Feb 2025
2	MPI	Update to 2.7	CEO	Feb 2025	Feb 2028

Contents

1. Introduction

1.1. Aim and purpose

This policy is designed to give guidance on the use of personal IT devices accessing Trust data and the use of such device for work purposes. It also aims to protect children from harm, minimise risk to the school networks and explain what constitutes acceptable use of the Bring Your Own Device (BYOD).

1.2. Application

This policy applies to all Leger Education Trust staff, students, governors, volunteers, visitors and contractors.

2. Policy

2.1. Definition of BYOD

A BYOD is personal owned piece of IT equipment i.e., not owned by the Trust. It includes but not limited to the following devices:

- Laptops and computers
- Smart phones
- Tablets such as iPads and eReaders
- USB Data Sticks
- Cameras and audio recording equipment
- Any electronic device that can connect to Trust ICT network

2.2. Definition of Trust Data

Trust data is any information that belongs to the Trust this includes but no limited to electronic files, images, videos, databases and emails. This data may be stored onsite on the Trust servers or may be with a 3rd party supplier to the Trust e.g. Microsoft 365

2.3. Lost, Stolen, or Damaged Devices

The Trust takes no responsibility for stolen, lost, or damaged devices, lost or corrupted data on those devices, this includes infections from viruses and malware. Although the Trust takes many measures to protect the network and the devices attached to it from viruses and malware.

2.4. Usage Costs

The Trust is not responsible for any costs incurred during work related use. For example, using your mobile data (3G/4G/5G) on your smartphone to access emails.

2.5. Acceptable Use

Staff and visitors participating in BYOD must adhere to the Trust's: -

- Acceptable Use Policy and
- Safeguarding Policy

Additional requirements for BYOD: -

- Cannot be used in toilets, bathrooms and changing rooms.
- Should not be used for contacting pupils, parents, or carers, unless it is an emergency, or they are unable to use the Trust telecoms systems.
- Cannot be used to take pictures or videos of pupils.
- But can be used to take pictures/videos of schoolwork, which is then transferred to the Trust ICT systems, but it must not contain images of the pupils. It then should be then removed from the BYOD.
- They should not be used store Trust data e.g. files, images, videos. BYOD devices are there to access and process information e.g. Email, Microsoft 365, watch video stream.

- Should a BYOD device become lost that had access to Trust data, you must inform the IT dept as soon as practicable. This is so Trust data can be secured, by changing passwords or blocking remote access.

2.6. Security

To protect Trust data where applicable the BYOD should be: -

- Protected with either password or PIN
- Data stored in an encrypted format e.g. Bit locker.
- Protected with anti-virus, anti-malware, and firewall software.
- Kept up to date with security patches and software updates.

For example, if you access your webmail from your PC at home, and you did not have any Anti-Malware on your PC, you could easily have a "key logger" that could then steal your username and password for your account as you signed in.
Failure to adequately protect your device will exclude you from using your device to access Trust data.

2.7. Network Access

If a BYOD requires internet access, it should only connect the Guest Wi-Fi network which is current named "LegerGuest", of the Trust only. It should not connect to other Trust Wi-Fi networks even if visible.

Access to the "LegerGuest" WiFi is given by a one time use 8 digit code, which can provide access for either 1 day or 30 days. The 1 day codes are typically used for external visitors to site and these codes can be acquired via reception or the School Business Managers. The 30 day codes can be obtained from the IT Department and typically reserved for staff use or post 16 students.

The Trust reserves the right to not allow your BYOD access to the Guest Wi-Fi if it deems your device as being unsecure or believes you will misuse the network.
All internet access is recorded, logged, and filtered for BYOD devices that are using the Trust's Wi-Fi network.

2.8. Charging the device onsite

The device's charger must be PAT tested and certified by Trust before being plugged into an electrical socket on the Trust site.
Devices may be charged with a suitable USB cable plugged in to a Trust provided device e.g. USB Charge Point, but the Trust takes no responsibility if the device is damaged or data lost in using such a facility.

2.9. Confiscation

If a student breaches the BYOD Policy or if a member of staff feels that they are likely to have breached this policy, then the student's device will be confiscated and held in the school office until the end of the day. The student's parents/carers may be contacted.

3. Signed Declaration

Please complete the section below to show that you have read, understood and agree to the rules included in the BYOD policy and also the Acceptable Use Policy and Safeguarding Policy. If you do not sign this agreement, access will not be granted to BYOD.

I have read and understand the above and agree that when using my personal IT device onsite or to access Trust data to abide by them.

Name Printed ……

Signed ……

Date ……