Langley Park Learning Trust

Use of Personally Owned ICT Devices (Bring Your Own Device) Policy

Owner (job role):	Data Protection Officer
Approval Body:	Resource and Finance Committee
Approval Date:	10 December 2020
Implementation Date:	1 January 2021
Review Date:	1 January 2022

Version	Approval Date	Summary of Changes

LPLT USE OF PERSONALLY OWNED ICT DEVICES (BYOD) POLICY

Introduction

This policy is in place for the occasions when staff or pupils use their own ICT equipment when dealing with data belonging to the Trust or one of its schools.

There is a small network of computers which are used in the administration of the Trust and its schools (finances, pupil records, timetables, registers etc). Many more computers are available for use by pupils and staff and the majority of these have access to the internet through the school network. All staff and pupils have a login name, password and an email account. The email system is available for use both from within the school and externally using a web browser.

Our IT service support contractor in conjunction with each school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access.
- No user should be able to access another's files without permission (or as allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the school's internal data security policy and as required by the General Data Protection Regulation (GDPR).
- Logs are maintained of access by users and of their actions while users of the system.

When staff or pupils use their own devices (eg. laptops, tablets, smartphones) it is imperative that:

- Normal IT use protocols are maintained.
- No vulnerabilities are introduced into the school's existing secure environments.
- Data protection matters are complied with.

Any queries regarding this policy should be addressed to the Trust's Central Team.

Objectives and targets

The objective of this policy is to develop an appropriate code of practice for the use of ICT by staff and pupils when using their own devices (BYOD).

Action plan

The following code of practice must be adhered to by staff and pupils who have the privilege of using BYODs to carry out their work. Not all staff and pupils will have this privilege.

All staff and pupils who are permitted to use BYOD at are expected to have read, understood and abide by the following policies, all available on the Langley Park Learning Trust website:

- This policy
- Online Safety policy
- LPLT Acceptable Use policy (this will appear whenever a person logs in)

All BYODs must have appropriate security in place, including anti-virus protection, and it must be updated regularly. It is the staff member's, pupil's or parent's responsibility to ensure this.

Periodic audits and checks on compliance will be undertaken by the school's network manager, who is also available to offer guidance on what is and is not acceptable use of BYODs.

Handling personal data (where Data Protection Act and GDPR apply)

Staff should aim to not routinely store or process personal data on BYODs. However, if this becomes necessary then any sensitive information held on BYODs and relating to the school must be accessible only by a password, PIN or encryption. This is to prevent personal data relating to school matters being accidentally or deliberately compromised or accessed by anyone other than the member of staff or pupil. This also applies wherever data is stored (eg on the device, portable hard drive, memory card, SD card, intranet or cloud). Such data may include:

- Information relating to staff, eg performance reviews.
- Pupil reports.
- SEN records.
- Letters to parents.
- Class-based assessments.
- Exam results.
- Whole school data.
- Medical information.

Care should always be taken to log out after each session to ensure that unauthorised access is not possible, eg in the event of the device being lost or stolen.

Members of staff / pupils should speak to the network manager about whether an encrypted channel could be set up to offer better security when transferring data of a secure nature from a BYOD to the school's network. Similarly, before using BYODs in cafes, hotels etc staff should seek advice from the network manager about the safety of such operations.

Where personal data relating to the school is stored on the BYOD, it should be deleted safely and securely as soon as it is no longer required. This also applies to data held on removable media eg USB drives.

When a member of staff / pupil leaves the school, s/he will be requested to remove all school-related data from any BYODs, having previously ensured that the school retains the data.

Handling other data relevant to the school

Where a BYOD is used for work purposes that do not involve personal data (and therefore have data protection implications) it is appropriate to maintain a clear separation of the work on the device from work which is of a confidential nature.

It is still important that school-related non-sensitive data held on BYODs must be accessible only by a password, PIN or encryption. This is to prevent data relating to school matters being accidentally or deliberately compromised or accessed by anyone other than the member of staff or pupil.

It is essential that any data not relating to school matters cannot be accidentally or deliberately uploaded to any device belonging to the school.

It is essential to be careful when installing any third-party software onto a BYOD. Untrusted sources have the potential to contain malware which could compromise any personal material belonging to the school. If in doubt, consult the network manager before uploading.

Members of staff / pupils are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Any images must only be taken on school equipment, never on personal equipment.

Use of Virtual Private Networks (VPNs)

VPNs are not be downloaded for use on BYOD in schools as these can cause school security systems to be bypassed.

Misuse of BYODs by staff / pupils

Misuse or abuse of the facility to use BYODs by staff or pupils is a serious matter and will be dealt with under the school's disciplinary procedures. The penalties for improper use may include dismissal either with or without notice.

Monitoring and evaluation

All use of BYODs at is a privilege. Senior leaders may request access to personal devices if they consider that this policy has been contravened, in order to investigate alleged abuse. The policy itself will be monitored and evaluated regularly, taking into account any incidents which occur or technological developments which might need a change in the policy.

Reviewing

The efficacy of the policy will be discussed annually as part of the Trustees' rolling programme of reviews.