BRING YOUR OWN DEVICES POLICY

The Learning Trust recognises that, as technology continues to evolve, many students now have access to personal internet-capable devices such as laptops, tablets, and mobile phones. These devices can offer significant educational benefits, allowing students and teachers to enhance learning, manage work effectively, and access a wide range of digital resources. However, the widespread availability of personal technology has also introduced new challenges within the school environment.

In response, the Trust has introduced a Bring Your Own Device (BYOD) Policy to provide clear guidance on the proper use of personal devices in schools. This policy must be implemented alongside each of our school's local Mobile Phone/Device Policy, which may vary depending on the context and specific needs of the school community. For example, in some schools, mobile device use is generally permitted, while in others, mobile phone use is restricted for students in Years 7–11 and allowed only in designated areas for Sixth Form students.

Where local school policy allows students to use mobile devices, these devices can connect to the filtered school wireless network, providing access to platforms like M365 and Google Classroom and other online resources.

Any staff or student use of devices must comply fully with both the school's Mobile Phone Policy and the overarching BYOD framework.

1. Conditions for Use / General Guidelines (where a school's policy permits use only)

1.1 Students and staff who wish to use a personally owned device, and access the school wireless network, therefore agree to, and accept the terms of this school policy and all acceptable use policies.

1.2 Use of personal devices on school grounds is at the discretion of teachers and staff. All students MUST use their devices as directed by their teacher and staff.

1.3 Access to the BYOD wireless network will be regarded as a privilege and not an entitlement and defined by the local school mobile phone policy. Use of the wireless network will require users to comply with clear conditions and expectations.

1.4 Use of the network will be monitored carefully by the IT Support team.

1.5 When explicitly permitted by a member of staff (and only when so permitted), a personal device may be used in lesson to support the lesson objectives.

1.6 The purpose of the use of personal devices at school is strictly educational. Mobile devices can only be used for personal reasons if the student has been given permission by a teacher or another member of staff.

1.7 Users must protect their device using a pass-code, password, or biometric lock.

1.8 Users must not attempt to circumvent the school's network security and/or filtering policies. This includes setting up VPN, proxies and downloading programs to bypass security.

1.9 Users must not use such devices to record, transmit, or post any of the following: photos, audio, or video of any person(s) within school without the explicit permission of the person(s) involved.

1.10 The Trust/school reserves the right to inspect and check any device if there is reason to believe that a student has violated school policy or has engaged in other misconduct whilst using the device.

1.11 Users will be advised to keep their device with them at all times, unless confiscated for a breach of policy.

1.12 Users should not expect to be able to charge their own devices using electricity provided by the school. If permission is given by a teacher to charge a device, it should be strictly to support learning.

1.13 To conform to Health and Safety compliance, any defective or damaged devices should not be brought into the school.

1.14 Devices should be turned off if not in use during lessons. Devices should not be used during transit between lessons.

2. Classroom guidelines:

Personal devices should only be used in the classroom when explicitly allowed by staff. All users must follow the instruction given by any teachers regarding their use of a personal device.

3. Consequences for Sixth Form students and those with permission in KS3 and KS4:

See local school Mobile Phone/Device Policy

4. Filtering:

The Trust shall maintain appropriate filters on the school WIFI network to ensure that personal devices that connect to the school WIFI network for internet access have their content filtered. The Trust's filters will consist of blacklists of inappropriate sites and terms that will be blocked. If a blocked site is required for learning a request can be made to the IT Support Team, who will forward it to the appropriate parties to decide if the request is appropriate. This is reviewed and often other sites are added to the blacklist.

5. Logs:

The Trust will maintain logs of usage of its network. Students and staff should be aware that their usage will be contained within these logs and that usage can be inspected to ensure compliance with the school and Trusts' policies on online content.

6. Monitoring:

In accordance with our Acceptable Use Policy, for both staff and students, the Trust will monitor the use of the school systems. Reports of any concerning behaviour are made to the DSL or other relevant SLT staff. Any safeguarding concerns are reported directly to the DSL by telephone or email, depending on the urgency. The DSL follows up any safeguarding concerns with the

appropriate person and relevant pastoral staff, follow up behaviour concerns and breaches of the Acceptable Use Policy.

7. School Liability:

7.1 Users bring their devices to use at school at their own risk. Personal devices are often expensive items. Students and staff must keep their devices in a secure place when not in use. Users are advised to make sure they have suitable protection and/or insurance for the devices to protect against accidental damage, theft, or loss.

7.2 Users are expected to act responsibly concerning their own device, keeping it up to date with patches and software updates where appropriate. It is their duty to be responsible for the upkeep and protection of their devices.

7.3 The Learning Trust is not responsible for:

- personal devices that are broken while at school or during school-sponsored activities
- personal devices that are lost or stolen at school or during school-sponsored activities
- network costs incurred should the student not use the school-provided wireless network

7.4 Any damage or disruption to the Trust network caused because of improper use of a student or staff-owned device will be regarded as an extremely serious matter.

8 Personal Data:

8.1 The Trust has a legitimate basis on which to access and protect data stored or processed on devices, including the content of any communications sent or received from the device. However, the Trust recognises the need to balance our obligation to process data for legitimate purposes, with expectations of privacy in respect of your personal data. Therefore, when taking (or considering taking) action to access your device or delete data on your device (remotely or otherwise) in accordance with this policy, the Trust will, where practical:

- consider whether the action is proportionate given the potential damage to the Trust, school, our customers or other people impacted by this data;
- consider if there is an alternative method of dealing with the potential risks' interests (recognising that such decisions often require urgent action);
- take reasonable steps to minimise loss of your personal data on your device, although we shall not be responsible for any such loss that may occur; and
- delete any such personal data that has been copied as soon as it comes to our attention (provided it is not personal data, which is also school data, including all personal emails sent or received using our email system).

8.2 To reduce the likelihood of the Trust or school inadvertently accessing students', staff, and/ or third parties' personal data, you must follow the following steps to separate school data from your personal data on the device:

- organise files within the device specifically into designated folders that clear data and personal data (for example, marking your own folders as “PERSONAL”).
- only use recommended official applications, such as one Microsoft OneDrive, when working on school files.
- do not use school email for personal purposes, but if you do ensure that is labelled appropriately in the subject line.
- regularly backup all personal data stored on the device.

9. Individual Healthcare Plan (IHP)

- Every diabetic student using a mobile device for medical purposes should have an Individual Healthcare Plan (IHP).
- The IHP must detail:
    i. The type of diabetes technology used (e.g., CGM, insulin pump).
    ii. The role of the mobile phone in managing their condition.
- Any alerts or alarms that may occur during the school day
- Students must have continuous access to their mobile device:
    - Within 6 meters of their person at all times 2.
    - Even during exams, assemblies, and breaks.
- **Vibration alerts** should be used to minimize disruption, except for urgent low glucose alarms which cannot be muted
- Devices should be registered with the school and students should be given a pass that states that their phone can be used as medical equipment.
- Liaise with the IT Team to ensure students can be connected to the school network
- Students must agree to use the phone only for medical purposes during school hours.
- Any misuse should be addressed with alternative sanctions, not removal of access
- Devices should be registered with the school and marked as medical equipment.
- Students must agree to use the phone only for medical purposes during school hours.
- Any misuse should be addressed with alternative sanctions, not removal of access