THE JUBILEE ACADEMY

Aspire and Achieve

Title:	**Mobile Technologies inc. BYOD/BYOT Policy**
Date Approved:	**December 2021**
Date Reviewed:	**September 2022**
Status:	**Non-Statutory**
Delegation:	**Head of School**
Responsibility:	**SBM H&S and IT Technician**
Review Frequency:	**Annually**
Policy Locations:	**Website/Staff Shared Drive/Hard Copy**
Next Review Date:	**September 2023**

Scope of the Policy

Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's cloud-based services such as email and data storage.

The absolute key to considering the use of mobile technologies is that the students, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned.

These mobile technologies policy sits alongside a range of polices including but not limited to the safeguarding policy, anti-bullying policy, acceptable use policy, policies around theft or malicious damage and the behaviour policy.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximising the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students that will prepare them for the high-tech world in which they will live, learn and work.

Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school 's network, filtering of personal devices, breakages and insurance, access to devices for all students/pupils, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership.

The school therefore allows the following **mobile technology implementations**:

	School/ devices		*Personal devices*			
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	**No**	**Yes**	**Yes**
Full network access	***Yes***	***Yes***	***Yes***	**No**	**No**	**No**
Internet only	**Yes**	**Yes**	**Yes**	**No**	**Yes**	**Yes**

- The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices (delete/amend as appropriate):
    - All school devices are controlled though the use of monitoring software and go through the school's web filtering to monitor use and help prevent students accessing inappropriate material;
    - Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g. Internet only access, network access allowed, shared folder network access)
    - The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
    - For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
    - Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licensed software etc.
    - All school devices are subject to routine monitoring
    - Pro-active monitoring has been implemented to monitor activity

- When personal devices are permitted:

    - We advise against bringing mobile phones to school. All student mobile phones and other electronic devices are collected every morning and stored safely until end of day when they are returned to students
    - All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access
    - Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user as does the liability for any loss or damage resulting from the use of the device in school
    - The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
    - The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
    - The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Passcodes or PINs should be set on personal devices to aid security
    - The school is not responsible for the day-to-day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues

- Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;
    - Devices may not be used in tests or exams

- Visitors should be provided with information about how and when they are permitted to use mobile technology in line with External agency Acceptable user agreement
- Users are responsible for keeping their device up to date through software, security and app updates. The device must be virus protected and should not be capable of passing on infections to the network
- Users are responsible for charging their own devices and for protecting and looking after their devices while in the school
- Personal devices should be charged before being brought to the school as the charging of personal devices should not take place using school resources
- Devices must be in silent mode on the school site and during all school activities
- School devices are provided to support learning.
- Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted
- The software/apps originally installed by the school must remain on the school owned device in usable condition and be always easily accessible. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
- The school will ensure that devices contain the necessary apps for schoolwork. Apps added by the school will remain the property of the school and will not be accessible to students on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
- Where photos are to be taken of activities involving students a school issued technology should be used rather than personal technology;
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances
- Printing from personal devices will not be possible
- The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden and will be dealt with in accordance with the school's behaviour and preventing and responding to bullying policies;
- Students are not permitted to use the cameras in their mobile phones at any time;
- Senior staff will have access to the unify app that enables phone calls from the school number be made via the staff mobile phones
- Staff going on a trip will be issued with a school mobile phone where contact with students is necessary;

School Equipment

1. What strategies are there in place for preventing damage, theft and loss?

All mobile devices

- Marked as TJA property with security sticker.
- When purchased they are added to a spreadsheet inventory which lists all the devices owned by the school, who has possession of those devices, their ID number and the Serial Number of the device.
- A check is done on every device each time it is given out and upon return. When students use laptops, the staff member supervising is given a sheet which details any prior damage and leaves room for the recording of names of students who use each laptop.
- Clear guidelines are given to staff half termly in regards to the booking, monitoring and care of mobile devices.

Students

- All tablets are given to students in a protective hard book covering to protect the tablet when in use.
- All students and their parents sign an acceptable use before they are given a tablet or a laptop to use. This contract explains how students need to look after the tablet and their liability should the tablet be damaged.
- On receiving their device all students are given training on how to maintain and look after their tablet.

Staff

- All Staff tablets are given in a protective case; laptops, when taken off site, are given in a protective bag.
- All Staff sign the ICT Acceptable agreement when they are given a tablet or laptop which explains what they need to do to look after their device.

2. What strategies are in place for monitoring the condition of the mobile devices?

- The school carries out a regular audit of the staff devices and asks a sample of staff to bring in their device so that they can be checked.

3. What happens if a mobile device is lost or damaged

Students

- Parents are informed via a phone call and a letter.
- If a device requires a replacement part due to damage caused when in the child's care parents are charged the cost to replace the part (Exceptions may be given based on the financial situation of the family involved)
- If a device is damaged beyond repair or is lost when in the child's care parents are charged the cost to replace the device (Exceptions may be given based on the financial situation of the family involved

Staff

- The Head of Department is informed.
- Payment of the insurance excess is taken from the departmental budget.

4. What happens if a mobile device is accidentally damaged or not working

Students

- Staff notify the IT technician via email and on any sheets provided with the device. The device is checked, then if damaged/broken, logged on the inventory as damaged/broken
- IT will attempt to fix the device
- If the device cannot be repaired by the IT technician, parents are informed via a phone call and a letter
- Parents are asked to contribute £20 toward the insurance excess.
- Finance is informed and a payment option is set up.

Staff

- Staff take the device to the IT technician who will attempt to repair.
- If the device cannot be repaired by the IT technician, the Head of Department is informed, and the insurance excess is taken from the staff/departmental budget.