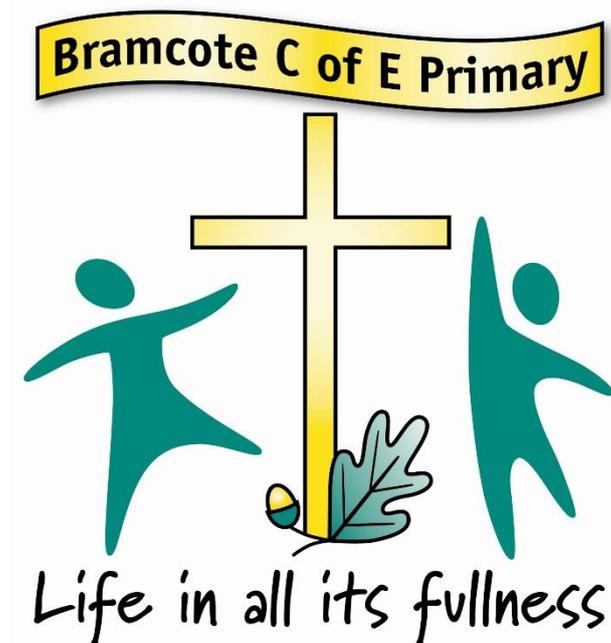


BRAMCOTE C OF E PRIMARY SCHOOL



MOBILE TECHNOLOGIES POLICY

SEPTEMBER 2020 - 2021

Mobile Technologies Policy

Mobile technology devices may be a school owned 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 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 pupils, 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. The mobile technologies policy should sit alongside a range of policies including but not limited to the safeguarding policy, anti-bullying policy, acceptable use policy, and the behaviour policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

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 maximizing 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 pupils 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 network, filtering of personal devices, breakages and insurance, access to devices for all pupils, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership

Schools may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.

The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

- The school acceptable use agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies
- Only School provided mobile devices e.g. iPads, access to the school Wi-Fi and network.

| | School/academy/devices | | | Personal devices | | |
|---------------------|---|--|--------------------------------|-----------------------|-------------|---------------|
| | School/academy owned and allocated to a single user | School/academy owned for use by multiple users | Authorised device ¹ | Pupil/Student owned | Staff owned | Visitor owned |
| Allowed in school | Yes | Yes | Yes | Yes with restrictions | Yes | Yes |
| Full network access | Yes | Yes | Yes | No | No | No |
| Internet only | Yes | Yes | Yes | No | No | No |
| No network access | Yes | Yes | Yes | No | No | No |

- The school/academy has provided technical solutions for the safe use of mobile technology for school/academy devices/personal devices (delete/amend as appropriate):
 - All school devices are controlled through the use of encryption software for staff laptops per user basis, curriculum devices are managed by encryption which prevents copying of data to external /portable devices. Ipad have passcodes or biometric unlock.
 - 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 is delegated by user name which is different for staff and pupils and they have different permissions on the network)
 - 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.
 - *All school devices are subject to routine monitoring*
 - *Pro-active monitoring has been implemented to monitor activity*
- *When personal devices are permitted:*
 - *All personal devices are restricted and no Wi-fi, Network access is permitted*
 - *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 (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school*

¹ Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the 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/academy 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. Pass-codes 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 users 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
 - Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
 - Users are responsible for keeping their device up to date through software, security and app updates. The device is 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 is not permitted during the school/academy day
 - Devices must be in silent mode on the school site
 - 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 easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Regular 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 school work. 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/academy 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

- *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*

Insurance

Devices are only insured via the LA insurance scheme whilst on school property,

Copyright of the SWGfL School Online Safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2020. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal/professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.