Clyro Church in Wales Primary School

Mobile Devices Policy

Policy agreed: 21.06.19

Policy to be reviewed: June 2021

Signed (Head teacher)

Signed (Chair of Governing Body)

Clyro C In W Primary School Policy

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

The absolute key to considering the use of mobile technologies is that the learners, 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/college owned/provided or personally owned. The mobile technologies policy should sit alongside a range of polices including but not limited to the safeguarding policy, anti-bullying policy, acceptable use agreement, policies around theft or malicious damage and the behaviour policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

A policy that completely prohibits pupil/student, staff or visitors from bringing mobile technologies to the school/academy could be considered to be unreasonable and unrealistic for school/academy to achieve. For example many parents/carers would also be concerned for health and safety reasons if their child were not allowed to carry a mobile phone and many staff and visitors use mobile phones to stay in touch with family. Contractors require mobile technologies for legitimate business reasons.

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. Learners 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 learning, but they can also develop digital literacy, fluency and citizenship in learners that will prepare them for the high-tech world in which they will live, learn and work.

For further reading, please refer to "Bring your own device: a guide for schools" by Alberta Education available at: http://education.alberta.ca/admin/technology/research.aspx and to the " NEN Technical Strategy Guidance Note 5 – Bring your own device" - http://www.nen.gov.uk/bring-your-own-device-byod/

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

Schools/colleges 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.

A range of mobile technology implementations is possible. Schools/colleges should consider the following statements and remove those that do not apply to their planned implementation approach.

- **The school/college 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**
- **The school/college has provided technical solutions for the safe use of mobile technology for school/college devices and for personal devices**
- **For all mobile technologies, filtering will be applied to the school/college internet connection and attempts to bypass this are not permitted**
- **Where mobile broadband (e.g. 3G and 4G) use is allowed in the school /college, users are required to follow the same acceptable use requirements as they would if using school/college owned devices.**
- **Mobile technologies must only be used in accordance with the law**
- **Mobile technologies are not permitted to be used in certain areas within the school/college site such as changing rooms, toilets and swimming pools.**
- **Learners will be educated in the safe and appropriate use of mobile technologies as part of the online safety curriculum**
- The school acceptable use agreements for staff, learners, parents and carers will give consideration to the use of mobile technologies
- The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems)

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

School devices

- **All school devices are controlled though the use of mobile device management (MDM) software**

[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

- **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)**
- **All school/college devices must be suitably protected via a passcode/password/pin (and encryption where relevant). Those devices allocated to members of staff must only be accessed and used by members of staff**
- **Appropriate exit processes are implemented for devices no longer used at a school/college location or by an authorised user**.
- **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. Periodic checks of devices will be made to ensure that users have not removed required apps**
- **The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain their property and will not be accessible to learners on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs**
- **The school is responsible for keeping devices 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. Where user intervention or support for this process is required, this will be made clear to the user**
- **School devices are provided to support learning. It is expected that learners will bring devices to school as required**
- **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 is not permitted**
-

Personal devices

When personal devices are permitted:

- *All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of filtered 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 (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in the school/college*
- *Staff personal devices should not be used to contact learners or their families, nor should they be used to take images of learners*
- *The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at the 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 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*

User behaviour

Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;

- **The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the discipline/behaviour policy**
- **Guidance is made available by the school to users concerning where and when mobile devices may be used**

Visitors

Visitors are provided with information about how, where and when they are permitted to use mobile technology on the site, in line with local safeguarding arrangements when they sign into school. They are also informed about the school policy on taking images.

Residential settings

No pupil personal devices allowed on residential trips.