Hywel Dda Primary School
Use of Mobile Technologies Policy
September 2025

Version Control:

Version	Last Modified	Last Modified By	Document Changes	Date presented to and agreed by Governing Body
1	July 2025	James Jones	Full update	

UNCRC:

16. Protection of privacy

Every child has the right to privacy. The law must protect children's privacy, family, home, communications and reputation (or good name) from any attack.

17. Access to information

Children have the right to get information from the Internet, radio, television, newspapers, books and other sources. Adults should make sure the information they are getting is not harmful. Governments should encourage the media to share information from lots of different sources, in languages that all children can understand.

Use of Mobile Technologies Policy

Mobile technology devices may be a Hywel Dda Primary School owned/provided or privately-owned smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail 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 owned/provided or personally owned.

The 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. 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 resilience, fluency and citizenship in learners 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 learners, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership. 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. The school should consider the following statements and remove those that do not apply to their planned implementation approach.

- The school acceptable use agreements for staff, learners and parents/carers will consider the use of mobile technologies
- The school allows:

	School owned and allocated to a single user	School owned for use by multiple users	Authorised device[1]	Learner owned	Staff owned	Visitor owned
Allowed in the school	**Yes**	**Yes**	**Yes**	Yes	Yes	Yes
Full network access	*Yes*	*Yes*	*Yes*	No	No	No
Internet only				Yes – on limited occasions	Yes	Yes
No network access						

- 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,

---

[1]

removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.

- 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 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 into 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
- 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. 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 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 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 day
- Devices must be in silent mode on the school site and on school buses

- School devices are provided to support learning. It is expected that learners will bring devices to the 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 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. 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 school work. Apps added by the school will remain the property of the school 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.
- 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
- Devices may be used in lessons in accordance with teacher direction
- 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