



St Peter's Catholic Primary School



Policy	Bring Your Own Device (BYOD) Policy v2
Date Approved/Approving Body:	29.11.23
Signed – Chair of Governors:	L Murphy
Date of Next Review:	November 2025

'Loved by Jesus, we love, we learn, we live and grow together for Him'

Devices

The policy will include usage of the following devices; smartphones, other mobile/cellular phones, tablet computers, portable media devices, PDA, ultra-mobile PCs (UMPCs), laptop/notebook computers, including home desktops, wearable technology and any personally-owned device capable of storing corporate data and connecting to a network.

Services

The organisation will provide access to the appropriate range of services which are suitable for access by personal consumer devices. The services made available may be limited by information security concerns, technical complexity or undue cost.

User Responsibilities

Users approved to connect personal devices do so on the following conditions:

- Users are required to comply with the relevant organisational policies and standards. These include standards for user identification and passwords. This may be recorded in a written declaration.
- The user is responsible for all call and data tariffs for their connected device(s).
- Any additional charges incurred as a result of receiving corporate data are to be borne by the user.
- Users are responsible for the backup of their devices.
- Users must notify the organisation of any loss or change of ownership of the device using the standard reporting procedures.
- Users agree never to disclose their password to anyone and passwords are not to be stored unencrypted on the device.
- All users are responsible for the physical security of their own device; this includes passwords, encryption and physical control whenever they contain enterprise data.

- The use of a personal device is not to be a distraction in any way to teachers or to students, they must not disrupt class or study areas in any way.
- Staff shall not distribute pictures, video or any other material relating to students on their personal social media, this could include emailing/texting/twitter which is now 'X'/Instagram/facebook/Whatsapp etc or posting online.
- Staff shall not distribute work related pictures on their personal social media, this could include pictures, video or any other material relating to staff in their professional capacity, this could include emailing/texting/twitter which is now 'X'/Instagram/facebook/Whatsapp etc or posting online without prior permission from the individual and the school.
- The use of any personal ICT device in school is a privilege not a right and should not be used during lessons and working time for personal use.
- Staff should ensure confidentiality of data held on their personal device, consider who they share the device with and take measures to ensure security of that data.
- Photos and videos taken of **pupils** for work purposes must not be taken on a personal device. School ipads are supplied for this purpose.
- Photos and videos taken of **staff** for work purposes, should be taken on a work device, but if a personal device is used they must be transferred to the school network and be deleted from the personal device within five days. Data on personal devices may also be set to automatically back up to a personal cloud, this must also be checked, and data deleted within five days.
- If using a personal laptop/computer to process school sensitive data it must be saved onto the supplied encrypted memory stick and not saved to the laptop/computer drive.

Organisational Responsibilities

The organisation:

- will not manage the personal use of staff owned devices
- will not provide specific device support for staff owned devices.
- may collect application usage information for information purposes only from work devices.
- will have no visibility of personal data on the device other than installed applications
- will have no ability to uninstall applications on the device
- will remove access to remote and local services in the event of device loss, change of ownership, termination of employment or at the request of the user.

Enforcement

Any individual member of staff who contravenes this policy or jeopardises the security of the organisation's information is liable to disciplinary action and, where appropriate, legal action may be taken.

Staff are not permitted to use personal devices, including wearable technology, to covertly record (visual or audio) anyone in school. In the event of any recordings legitimately taking place the recordings are school confidential and the school will monitor content if it is deemed necessary. Failure to comply could result in disciplinary procedures.

Supporting documentation used by school to support the BOYD Policy:

ico. Bring your own device (BOYD): https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf