Woodbridge Primary School
Bring Your Own Device (BYOD) Policy

	Signed	Date
Approved by	**Matthew Gowen Chair of Governors**	**June 2022**
Last reviewed		**June 2022**
Next review due on		**June 2023**

Signed by: MATTHEW GOWEN **Chair of Governors**

Signed by: KATE DALY **Headteacher**

Our school promotes the positive use of technology in school. We recognise that these can be valuable tools for staff, governors and visitors but require that they are used in an acceptable way. This policy addresses the use of personal devices in school or at home for work purposes. These personal devices could include mobile phones, laptops, tablets, smart watches and personal computers. This policy supports the school's 'Acceptable Use' policy.

1. Use of mobile devices at the school

Staff and visitors must only use personal mobile devices to make and receive calls in specific places e.g. staffroom, workroom, office etc. where pupils are not present.

Staff and visitors to the school are responsible for their own mobile devices at all times.

The school is not responsible for the loss, theft of, or damage to the mobile device.

Mobile devices must be turned off or switched to silent mode during directed time with pupils.

Personal mobile devices must not be used to contact parents or pupils.

Personal devices must not be used to take photos, videos or sound recordings of the pupils or used by pupils.

2. Access to the school's Internet connection

The school provides wireless Internet which has a limited capacity and is therefore only for the connection of school devices. Personal devices must not be connected to the school's internet service.

3. Access to school services

Staff are permitted to connect to or access the following school IT services from their mobile devices or personal computers for the following purposes:

- to access the school email system
- to access the school virtual learning environment (Google Classroom)
- to access platforms such as Office 365 and Google Drives when working at home.

Staff must not store school data on their personal devices, or on cloud storage linked to their personal devices. If it is necessary for staff to download school information to

their mobile or personal devices in order to view it (for example, to view an email attachment), staff must delete this information from their devices as soon as they have finished viewing it.

Staff must not send school information to their personal email accounts.

4. Security of staff devices

Staff must take sensible measures to prevent unauthorised access to their personal mobile devices. This includes using a PIN, pattern or password in order to unlock the device, and ensuring that the device auto-locks if inactive for a period of time.

See also: **Acceptable Use Policy**