THE MARIST SCHOOL

Bring Your Own Device to School (BYOD) Policy for staff, volunteers, visitors and 6th form pupils

DfE No: 868/6013

Ratified Date: September 2018

Review Date: September 2020

Signed:

Ann Nash
Chair of Governors

Karl McCloskey
Principal

The charity of the order of the Marist Sisters Province of England (charity no. 225485) aims to promote and provide for the advancement of education by conducting and governing a day school for girls in England. The teaching shall be in full accordance with the Roman Catholic Church.

Bring Your Own Device (BYOD) Policy for Marist School staff, volunteers, visitors and 6th form pupils

The Marist School recognises that digital technology offers valuable benefits to staff from a teaching and learning perspective and to visitors on official business. The school embraces this technology, but requires that it is used in an acceptable and responsible way.

This policy is intended to address the use by staff members, volunteers and visitors of non-school owned electronic devices, to access the internet via the school's internet connection, to access or store school information, or to make photographs, video, or audio recordings at school.

These devices include, but are not limited to, smart phones, tablets, laptops, wearable technology and any similar devices. If you are unsure whether your device is captured by this policy please check with the Bursar. Throughout this policy, any such device is referred to as 'mobile devices' and supports the Acceptable Use of Technology Policies.

Use of mobile devices at the school

Staff and visitors to the school are responsible for their mobile device at all times. The school is not responsible for the loss, theft of, or damage to, any mobile device or storage media on the device (e.g. removable memory card) that may be caused whilst on the school premises.

Mobile devices must be turned off when asked or at appropriate times and must not be taken into controlled assessments and/or examinations, unless any special circumstances apply which must be discussed in advance with the relevant member of staff.

The school reserves the right to refuse staff and visitors permission to use their own mobile devices on school premises, should they feel that this is a necessary intervention.

Use of cameras and audio recording equipment

Parents and carers may take photographs, videos or audio recordings of their children at school events for their own personal use. However, these photographs and/or recordings must not be shared or posted on any social media whatsoever.

Other visitors and staff may use their own mobile devices to make photographs, video, or audio recordings in school provided they first obtain permission from the Bursar and that relevant permissions have been checked and obtained in advance. This includes people who might be identifiable in the background.

No one must use mobile devices to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely to take photographs, video, or audio recordings in school. Staff must comply with the school's social Acceptable Use of Technology Policy when making photographs, videos, or audio recordings.

Access to the school's internet connection

The Marist School provides a wireless network that staff, visitors and some pupils may use to connect their mobile devices to the Internet. Access to the wireless network is at the discretion of the school, and the school may withdraw access from anyone it considers is using the network inappropriately.

The school cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk. In particular, staff and visitors are advised not to use the wireless network for online banking or shopping.

The school is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the school's wireless network. This activity is taken at the owner's own risk and is discouraged by the school. The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's wireless network.

Access to school IT services

Marist School staff are permitted to connect to or access the following school IT services from their mobile devices:

- the school email system;
- the school virtual learning environment (FROG);
- OneDrive, and any other Microsoft 365 application.

Staff may use the systems listed above to view school information via their mobile devices, including information about pupils. Staff must not store the information on their devices, or on cloud servers linked to their mobile devices. In some cases it may be necessary for staff to download school information to their mobile 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 only use the IT services listed above, and any information accessed through them, for work purposes. School information accessed through these services is confidential, in particular information about pupils. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to or distribution of confidential information should be reported to the school's IT team or HR department as soon as possible.

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

If in any doubt a device user should seek clarification and permission from the school's Bursar before attempting to gain access to a system for the first time.

Monitoring the use of mobile devices

As detailed in the Acceptable Use of Technology Policy, the school can, and does, regularly monitor the Internet traffic in, through and out of its network.

Should any inappropriate activity be identified or reported via the use of a mobile device, the same disciplinary procedures will be followed and will be assessed on a case by case basis.

Security of mobile devices

Staff and pupils who are permitted to bring their own device into school must take all sensible measures to prevent unauthorised access to their mobile devices, including but not limited to the use of a PIN, pattern or password to be entered to unlock the device, and ensuring that the device auto-locks if inactive for a period of time.

Staff and pupils must never attempt to bypass any security controls in school systems or others' own devices.

You must ensure that appropriate security software is installed on their mobile devices and must keep the software and security settings up-to-date.