MAGDALEN COLLEGE SCHOOL

BRING YOUR OWN DEVICE (BYOD) POLICY

Non-Statutory Policy – Annual Review

GOVERNORS' EDUCATION & WELFARE COMMITTEE

Date next due for review by committee	Reviewed by committee	Any Changes YES/NO	Approved by Full Governors
New	24 April 2024	Yes	Approved by Committee 11 June 2024

Contents

---

1. Aims

The aims of this policy are to ensure that use of personal ICT equipment used in relation to school business meets the same standards of safeguarding of pupils, staff and the school as for school-owned equipment.

2. Scope of this policy

There are several situations where equipment which is not owned by the school is used in relation to school business:

a) Staff using a device which is not owned by the school whilst at school for their work as an alternative to using school equipment.
b) Staff using a device which is not owned by the school for personal use whilst on school premises.
c) Staff using a device not owned by the school whilst away from the premises in connection with their work.
d) Pupils using a device not owned by the school whilst on the premises or elsewhere in connection with their studies or otherwise.
e) Visitors using devices not belonging to school whilst visiting school.
f) Where this policy refers to "computer" this term is used generically to include smart phones, tablets, laptops and desk top computers.

3. Potential risks against which this policy mitigates.

- Bringing onto school premises unacceptable material or compromising personal privacy of staff
- Compromising confidentiality in relation to school information outside of the school
- Infecting school systems with electronic viruses and other similar threats
- Claims by users against the school for loss or damage to personal devices whilst in use for school business and/or whilst on the school premises.

3. Pupils' use of their own devices

Only those pupils in the sixth form are permitted to use their own computers whilst in school and they must:

a) only connect to the guest WIFI network whilst in school and never attempt to connect to other school networks or use the guest network whilst not on the premises.
b) ensure that their device has up to date (supported) operating systems and appropriate anti-virus software (approved by the school) installed to reduce risks of virus infection when connected to the guest network.
c) only use the device in lessons with the permission of the teacher, and only for the purposes of their work, or in the TGC or Library during study periods or break times.

d) not make any attempts to circumvent the school's network security at any time, including the setting-up of VPNs or proxies and use of programs to bypass security.

e) accept responsibility for their own equipment and accept that the school will, in no circumstances, accept liability for any loss or damage to equipment not belonging to the school whilst on the premises or in use for schoolwork.

4. Staff use of their own devices

For personal use

Staff are permitted to bring personal devices (e.g. mobile phone) into school for personal use. These should not be used whilst in contact with pupils (staff should not use their personal devices, for example, around the site, but should confine this to a staff room or empty classroom, for example).

For use in connection with their work

All staff who are required to use a computer in connection with their work are provided with access to a suitable device by the school. If a member of staff wishes to use their own device in connection with their work, they may only do so provided the following conditions are met:

a) the device is free from material which compromises the school's acceptable use policy.

b) they give permission to the ICT technical staff to inspect the device to ensure that these safeguards are in place.

c) no school information is stored on the device itself and storage of school information is cloud-based in the school's cloud storage accounts (i.e. it is not permissible to store school information in cloud storage owned by or subscribed to by the member of staff personally).

d) password protection is in place to protect school information whilst the device is in school and away from the premises. This includes, for example, the protection of passwords for school systems (e.g. Go4S) to prevent unauthorised access to these systems whilst the device is in and out of school.

e) the device is not used by anyone other than the member of staff or, when used by anyone other than the member of staff a different log in profile is used to prevent unauthorised access to school information and systems.

f) not make any attempts to circumvent the school's network security at any time, including the setting-up of VPNs or proxies and use of programs to bypass security.

g) accept responsibility for their own equipment and accept that the school will, in no circumstances, accept liability for any loss or damage to equipment not belonging to the school whilst on the premises or in use for school business.

5. Visitors

Visitors, including governors, may use their personal devices in connection with work at Magdalen. The same protocols set out for staff apply, however visitors may use the visitor WIFI network.

6. Links with other policies

All stakeholders must view this policy in the context of the Online Safety Policy, the Safeguarding and Child Protection Policy and the Data Protection Policy.