NEWCASTLE
SCHOOL
FOR BOYS

Bring your own device (BYOD) wireless network policy

Newcastle School for Boys (‘the School’) provides a bring your own device (BYOD) wireless network which is made available to staff and pupils who have a compatible wireless device to enhance their professional and educational activities including learning, teaching, research, administration and management.

Use of this provision is governed by the School’s ***BYOD acceptable use policy: terms and conditions***. By logging onto the School’s network, the user is deemed to have agreed to abide by both the ***School’s BYOD acceptable use policy: terms and conditions*** and Wi-fi Policy.

Any user utilising the School’s BYOD wireless network must be aware of and agree to conditions of use including, but not limited to the following:

1. The School assumes no responsibility for the safety of equipment or device configurations, security, or data files resulting from connection to the School’s BYOD wireless network or the Internet, nor liability for any damages to hardware, software or data, howsoever caused.

2. The School assumes no responsibility for providing any form of repair service for any personal device used on the BYOD wireless network.

3. BYOD wireless access is provided as a free service on an "as is" basis with no guarantee of service.

4. The BYOD wireless network provides basic data encryption between the access points and the end user device. Use of the BYOD wireless network for internet connection is undertaken at the user's own risk. It is the responsibility of the user to protect their wireless devices through use of up-to-date virus protection, personal firewall and any other suitable measures.

5. Access to the BYOD wireless network must only be made via the user’s authorised network username and password. Under no circumstances should these details be made available to any other person, including family. The authorised user will be held responsible for any inappropriate use of their named account.

6. A personal device should only be used on the BYOD wireless network by its owner and the device must not be loaned to any other person.

7. A user is restricted to one enrolled device. A registration form must be completed for that device prior to enrolment on the BYOD wireless network.

8. Personal devices must be enrolled and configured on the BYOD wireless network by a member of the School’s IT department.

9. Devices must be password protected and a working and up-to-date anti-virus product installed. Enrolment will be refused if no anti-virus product is present.

10. The School will install a certificate to connect the device to the School's internet filtering system. This filtering is only applied within the range of the School's BYOD wireless network.

11. Following enrolment, the School is capable of management of the devices but will not enforce any restriction policies upon the device.

12. Applications or programs installed on devices by the owner may not function through the School's BYOD wireless network. The School reserves the right to refuse requests to provide user access to these applications or programs on the School's network.

13. If the enrolled device is lost by the user, the IT School Network Manager must be notified as quickly as possible so that the device can be removed from the system.

14. Enrolment of the device will be terminated as soon as the user is no longer directly involved in the School. The guest wireless network provides basic data encryption between the access points and the end user device. Use of the guest wireless internet connection is undertaken at the user's own risk. It is the responsibility of the user to protect their wireless devices through use of up-to-date virus protection, personal firewall and any other suitable measures.

15. The BYOD wireless network may be subject to periodic maintenance and unforeseen downtime.

16. The School filters and monitors ALL Internet access. Misuse may lead to enrolment on the BYOD wireless network being terminated.

17. Printing access is not available via the BYOD wireless network.

18. Any attempt to circumvent School procedures, or any unauthorised attempt to access or manipulate School equipment or networks, may result in permanent disconnection from the BYOD wireless network and further disciplinary action being taken.

Changes to this policy

We may revise this policy at any time by posting the updated version of the policy on our site. You are expected to check this policy from time to time to take notice of any changes we make, as they are legally binding on you. Some of the provisions contained in this Policy may also be superseded by provisions or notices published elsewhere on our site.

September 2017