BRING YOUR OWN DEVICE POLICY (BYOD)

RGS

BRING YOUR OWN DEVICE POLICY (BYOD)

Newcastle upon Tyne Royal Grammar School

The Bring Your Own Device (BYOD) policy was introduced in connection with the provision of facilities in the Royal Grammar School Newcastle (RGS) for reliable and fast WiFi connection.

This reflects the increased use of personal devices (owned by individuals) by staff, students and visitors at school that are used in school and could connect to the school BYOD WiFi or guest WiFi networks.

The school is committed to supporting users of BYOD by means of:

- Its Staff and Student ACCEPTABLE USE POLICIES
- A school-wide enterprise level Wi-Fi network
- Appropriate filtering and blocking access to content deemed inappropriate to the setting.

Please see the paragraph at the end of this policy for additional rules and requirements applying to BYOD use.

When a personal device is used as a work tool to access the school systems and/or its data, the usual responsibilities apply. This includes security of the transfer of data between the personal device and the school system. The user takes full responsibility to safeguard data and the transfer of data. Staff and students seeking to use data (in particular sensitive personal data) held on the school's databases and files must only access them via their RGS Office 365 or iSAMS account. **Staff and students should not store confidential information** on the device itself and only access such data remotely.

All RGS policies relating to use of social media also apply when media is accessed via BYOD devices. All staff and students using BYOD are required to conform to expected standards of online behaviour and not download or transmit any material which might be harmful or offensive to any RGS student or member of staff or to members of their families, or bring the School into disrepute. Any breach of this protocol will be treated as a serious disciplinary matter. See the policies on SAFEGUARDING, SAFEGUARDING CODE OF CONDUCT, ANTI-CYBERBULLYING and ANTI-BULLYING for further details on use of social media.

The school will monitor the content of user-owned devices for threats to the technical infrastructure of the school. The school reserves the right to prevent access to the network by any device that is considered a risk and to access material which it has reason to believe has been used to harm an individual or the school in some way.

With regard to use of BYOD via the RGS WiFi network, the school will seek to manage this by means of filtering the risks surrounding:

- Accessing inappropriate web content
- Hosting of inappropriate services on user owned devices (e.g. illegal music or film download torrent services)
- The transfer of school data to third party storage facilities.

RGS will publish mandatory policies and user information for secure configuration of all BYOD devices. Any attempt to circumvent or subvert the school's security systems will be a disciplinary matter.

For further information contact the IDT Department (it.support@rgs.newcastle.sch.uk)

All RGS BYOD users should refer to the school's ACCEPTABLE USE POLICY and note the following additional rules and requirements relating to BYOD use:

- The user is responsible for the safe keeping, maintenance and insurance of the device at all times.
- All BYOD devices brought into school must only be connected to the RGS network via

software provided or approved by RGS.
• Users must keep their device's software up to date and ensure that no content threatens the integrity and security of the device.
• Users should not keep files relating to RGS on their device. These should be stored on their RGS Office 365 account.
• Users should

- delete from their device any sensitive school related emails and files (including email attachments) as soon as they have finished using them
- limit the number of school emails and other information they sync to their device to limit the possibility of inappropriate or excessive data transfer.
- In exceptional circumstances, where there is good reason to believe that a device has been misused in school or in connection with an RGS organised activity or with any RGS student or member of staff, the school reserves the right to have access to RGS related data or material kept on the device.
- RGS reserves the right to deny access to its network by any device reasonably considered to be a risk to the network and to remotely locate and wipe any unauthorised or inappropriate material.
- In the case of a BYOD device belonging to a student (or belonging to a relative or third party, but used in school by the student), RGS reserves the right to remove the device to secure storage pending further enquiries under disciplinary procedure; and the loss of any device holding data relating to the school or with access to the RGS network must be reported immediately to the IDT Department at it.support@rgs.newcastle.sch.uk and the owner must immediately change his/her password(s) for all access to RGS network services.
- Users should ensure that ythey don't agree to register the device with the School IT administrator if the user chooses to download Office 365 applications. This will result in the school IT administrators being able to manage certain apps.

This policy is supplementary to the policies for ACCEPTABLE USE POLICY FOR STUDENTS, ACCEPTABLE USE POLICY FOR STAFF and PRIVACY NOTICE, which apply when mobile devices are used within the school or on RGS-organised activities.

Click here to complete the acceptance form. By submitting the form you agreeing to adhere to the terms and conditions set out in the policy above.