Newcastle upon Tyne Royal Grammar School

Bring your own device policy

This policy applies to the whole school and is published to parents, students and staff

Updated August 2016 Author: Michael Pitkethly

The Bring our own device (BYOD) policy has been introduced in connection with the provision of facilities in the Royal Grammar School Newcastle (RGS) for reliable and fast Wi-Fi connection, reflecting the increased use of tablet devices (owned by individuals or provided by the School) by staff, students and visitors, and recognising that BYOD may become the accepted way to access IT services inside and outside the classroom.

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

- Its Acceptable use policy
- A school-wide enterprise level Wi-Fi network
- Information systems designed to operate on a range of user devices
- Automated scripts and security policies via mobile device management (MDM) systems and software
- Appropriate filtering and blocking access to content deemed inappropriate to the setting.

This policy is supplementary to the policies for Acceptable use of ICT for students and Data protection, both of which apply when mobile devices are used within the School or on RGS-organised activities. Please see the paragraph at the end of this policy for additional rules and requirements applying to BYOD use.

There is an additional Acceptable use of ICT for staff policy in the staff handbook.

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. Therefore RGS requires that MDM is installed on every tablet and mobile device when it connects to the School Wi-Fi network. Where MDM is not installed e.g. on laptops, then the user has the usual responsibilities to safeguard data and the transfer of data.

Staff seeking to use data (in particular sensitive personal data) held on the School's databases and files must only access them via Citrix (which provides a safe, secure virtual worktop that can be accessed from all platforms and does not store any data on the device itself) or by the Acronis Access app (available via the RGS MDM).

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 or 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 student use of BYOD via the RGS network, the School will seek to manage this by means of MDM and filtering the risks surrounding:

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

Given the risk of loss of the device itself together with any confidential data stored on it, even if all security procedures are followed, the RGS will seek to ensure best practice through MDM applications, including:

- A device lock code (4 digit PIN or complex password, the latter preferred)
- Automatic lock when idle
- Remote wipe capability
- Device data encryption
- The *locate my device* service (which is passcode protected).

RGS will publish mandatory policies and user information for secure configuration of all BYOD devices. Any attempt to circumvent or subvert the School's MDM (jail-breaking) will be a disciplinary matter. For further information contact the Director of IT Services, Paul Miller p.miller@rgs.newcastle.sch.uk

All staff, students and visitors using BYOD devices should read the additional Acceptable use points which apply to them. RGS recognises that BYOD is a dynamic advance, so it may be necessary to review and from time-to-time amend this policy to reflect new developments and issues regarding use.

Feedback from RGS BYOD users with regard to this policy and the Acceptable use policy is welcomed and should be sent to the Director of IT Service, Paul Miller p.miller@rgs.newcastle.sch.uk

All RGS BYOD users should refer to the School's *Acceptable use of ICT 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 device management 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 keep separate on their devices personal files and files relating to RGS*
- *Users should:*
    - *delete from their device any sensitive emails and files (including email attachments) as soon as they have finished using them; and*
    - *limit the number of 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 IT Support at* helpdesk@rgs.newcastle.sch.uk *and the owner must immediately change his/her password(s) for all access to RGS network services.*