Richmond Hill Primary Academy

Bring Your Own Device Policy

Created By:	K.Cousins
Date:	May 2017
Ratified By:	
Date:	

Policy Introduction

This policy covers the use of non-Academy owned electronic devices to access corporate systems and store Academy information, alongside their own data. Such devices include, but are not limited to, smart phones, tablets, laptops and similar technologies. This is commonly known as 'Bring Your Own Device' or BYOD.

If you wish to BYOD to access Academy systems, data and information you may do so, provided that you follow the provisions of this policy and the advice and guidance provided through the IT Technician alongside the SLT.

It is the Academy's intention to place as few technical and policy restrictions as possible on BYOD subject to the Academy meeting its legal and duty of care obligations.

Bring Your Own Device Policy

Executive Summary

This policy defines acceptable use by Academy users whilst using their own devices for accessing, viewing, modifying and deleting of Academy held data and accessing its systems.

Assumptions and Constraints

It is assumed that all staff at Richmond Hill Primary Academy have an awareness of the Data Protection Act (1998) and that they understand the consequences of the loss of Academy owned personal data.

Definitions

BYOD – Bring Your Own Device refers to Users using their own device (which is not owned or provided to by the Academy) to access and store Academy information, whether at the place of work or remotely, typically connecting to the Academy's Wireless Service.

Data Controller - The Data Controller is a person, group or organisation (in this case the Academy) who determines the purposes for which and the manner in which any personal data are, or are to be, processed.

User – A member of staff, enrolled student, contractor, visitor, or another person authorised to access and use the Academy's systems.

Richmond Hill Primary Academy remains in control of the data regardless of the ownership of the device. As a User you are required to keep Academy information and data securely. This applies to information held on your own device, as well as on Academy systems. You are required to assist and support the Academy in carrying out its legal and operational obligations, including co-operating with Information Systems should it be necessary to access or inspect Academy data stored on your personal device.

The Academy reserves the right to refuse, prevent or withdraw access to Users and/or particular devices or software where it considers that there are unacceptable security, or other risks, to its staff, students, business, reputation, systems or infrastructure.

The Academy takes Information and Systems Security very seriously and invests significant resources to protect data and information in its care.

The use of your own device MUST adhere to the Academy's Acceptable Use Policy which runs alongside the Staff Code of Conduct and Safeguarding Children and Young People's Policy.

In particular, when you use your own device as a work tool, you MUST maintain the security of the Academy's information you handle (which includes but is not limited to viewing, accessing, storing or otherwise processing).

From time to time, the Academy may require that you install or update Academy-approved device management software on your own device.

It is your responsibility to familiarise yourself with the device sufficiently to keep data secure. In practice this means:

- Preventing theft and loss of data (using PIN/Password/Passphrase lock)
- Keeping information confidential, where appropriate.
- Maintaining the integrity of data and information.

You MUST NEVER retain personal data from the Academy systems on your own device. If you are in any doubt as to whether particular data can be stored on your device you are required to err on the side of caution and consult with your manager, or seek advice from the SLT.

You MUST:

 Use the device security features, such as a PIN, Password/Passphrase and automatic lock to help protect the device when not in use.

 Keep the device software up to date, for example using Windows Update or Software Update services.

 Activate and use encryption services and anti-virus protection if your device features such services.

 install and configure tracking and/or wiping services, such as Apple's 'Find My iPhone app', Androids 'Where's My Droid' or Windows 'Find My Phone', where the device has this feature.

 Remove any Academy information stored on your device once you have finished with it including deleting copies of attachments to emails, such as documents, spreadsheets and data sets, as soon as you have finished using them.

 Limit the number of emails and other information that you are syncing to your device to the minimum required.

 Remove all Academy information from your device and return it to the manufacturers' settings before you sell, exchange or dispose of your device.

In the event that your device is lost or stolen or its security is compromised, you MUST promptly report this to the SLT, in order that they can assist you to change the password to all Academy services (it is also recommended that you do this for any other services that have accessed via that device, e.g. social networking sites, online banks, online shops). You must also cooperate with Academy officers in wiping the device remotely, even if such a wipe results in the loss of your own data, such as photos, contacts and music.

You MUST NOT attempt to circumvent the device manufacturer's security mechanisms in any way, for example 'jailbreak'1 the device.

Further advice on securing personal devices (including advice on the risks of downloading untrusted Apps) is available from the IT Technician.

Monitoring of User Owned Devices

The Academy will not monitor the content of your personal devices, however it reserves the right to monitor and log data traffic transferred between your device and Academy systems, both over internal networks and entering the Academy via the Internet.

In exceptional circumstances, for instance where the only copy of an Academy document resides on a personal device, or where the Academy requires access in order to comply with its legal obligations (e.g. under the Data Protection Act 1998, the Freedom of Information Act 2000, or where obliged to do so by a Court of law or other law enforcement authority) the Academy will require access to data and information stored on your personal device. Under these circumstances all reasonable efforts will be made to ensure that the Academy does not access your private information.

Under some circumstances, for example where you legitimately need to access or store certain types of information, such as student or financial records on your own device, you must seek authority from your Line Manager. The Academy may then need to monitor the device at a level which may impact your privacy by logging all activity on the machine. This is in order to ensure the privacy, integrity and confidentiality of that data.

The Academy takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding employee-owned devices, or for any loss or damage resulting from support and advice provided.

Use of Personal Cloud Services

Personal data as defined by the Data Protection Act (1998) and Academy confidential information may not be stored on personal cloud services.