Richmond upon Thames College

Policy Name:	Bring Your Own Device Policy (BYOD)
Policy Number/Version No:	V3
Effective Date:	April 2022
Review Date:	April 2023
Policy Responsibility:	IT Manager
Approved By:	SLT
For Action By:	All College staff and students
For Information to:	All College staff, students and parents/carers

1.0 Introduction

1.1 Richmond upon Thames College (RUTC) is dedicated to promoting our values of honesty, integrity, mutual respect and personal accountability to support our students in becoming fully rounded members of society with a strong sense of social and moral responsibility. We prepare our students for life in Modern Britain by developing an understanding of democracy, the rule of law, individual liberty, mutual respect and tolerance of those with different faiths and beliefs and this is reflected in our policies.

1.2 RUTC recognises the benefits that can be achieved by allowing staff, students and visitors to use non-college-owned devices such as mobile phones, laptops, and tablets to access and store college information as well as their own data. This practice is commonly known as 'bring your own device' or BYOD. RUTC aims to place as few technical restrictions as reasonably possible on the development and use of new applications and services, however the use of non-college-owned devices to process college information and data creates issues that need to be addressed.

1.3 RUTC provides a wireless network that is available for access by all users who have a compatible personal wireless device. The term 'Users' therefore includes any student, member of staff, governor or visitor. Use of this provision is governed by RUTC Computer Network, Internet, and Intranet Acceptable Use Policy, and by logging onto the network the user is deemed to have agreed to abide by the conditions of that policy.

RUTC has ownership of the corporate data and resources that may be accessed or stored on a device, but the device itself is the property of the user.

External guests can make use of RUTC's Cloud Path WIFI and will be provided details on how to join the network by the college reception staff. Access to the Cloud Path WIFI can be from one day to a whole year depending on the requirements of the external guest. The college reception will approve access and allocated the number of days required.

1.4 As a user you are required to assist and support the College in carrying out its legal and operational obligations with regard to college data and information stored on your device. You are required to co-operate with officers of the college when they consider it necessary to access or inspect college data stored on your device.

2.0 Conditions of Use

2.1 Any user utilising RUTC wireless connection and/or using a personal device, be that laptops, tablets, mobile phones, iPad's, Mac books, or gaming devices while in the College and/or when connecting to the College's computer networks should be aware of and agree to the conditions of use as set out in the Acceptable Use Policy and in the paragraphs that follow.

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

- Use the device security features, such as using biometrics, PIN or a strong Password/Passphrase 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 on a regular basis. RUTC requires all devices to be up to date before using the college WIFI, and older devices with outdated and unsupported Operating Systems

(OS) will not be allowed to connect. As per guidance from the NCSC, examples of out of date OS are:

    - Windows 7, and Windows 8
    - Any Windows 10 OS older than version 1909
    - Any mac OS older than 10.15: Catalina (Jazz) - 7
    - Any mac iOS older than 13.1
    - Any Android OS older than Android 10
    - Any Chrome OS older than 95.0.4638
    - Any Ubuntu LTS OS older than 20.04

- 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' Android's 'Android Device Manager' or Windows 'Find My Phone' where the device has this feature.
- Remove any College 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 synchronising to your device to the minimum required.
- Remove all College information from your device and return it to the manufacturers' settings before you sell, exchange, or dispose of your device.
- Whenever possible, use remote access facilities to access information on college systems. Log out and disconnect at the end of each session.

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

3.0 Terms of Reference

3.1 The College regrets it is not able to assume responsibility for the safety of personal equipment or device configurations, security, or data files resulting from connection to the College's wireless network or the Internet, nor liability for any damages to personal hardware, software, or data, howsoever caused.

3.2 Wireless access is provided as a free service on an "as is" basis with no guarantee of service (i.e., no expressed or implied level of coverage or performance is provided).

3.3 Users are responsible for setting up their own equipment to access the wireless network. A guide is available on the College's VLE, and from the IT Support Unit Room G19, to help users connect to the wireless network.

3.4 Staff will not be able to provide technical assistance or assume any responsibility for personal hardware configurations, security or changes to data files resulting from connection to the wireless network. It is recommended that users make a backup copy of any settings before configuring their equipment for use on the wireless network.

3.5 The wireless network provides basic data encryption between the access points and the end user device. Use of the wireless internet connection is undertaken at the user's own risk. It is the responsibility of the user to protect their wireless devices using up-to-date virus protection, personal firewall and any other suitable measures using secure browsers such as Edge, Chrome, and Safari including built-in password managers which are usable 'out of the box.' In combination with cloud services, RUTC has a requirement that all devices meet requirements outlined by NCSC.

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

3.7 The College filters and monitors ALL network and Internet access, including when accessed via a wireless connection, and reserves the right to take action where inappropriate use is observed.

3.8 Printing access is available via the wireless network users can use the emailtoprint@rutc.ac.uk option. Users will need to use their college account with MS Outlook application to be able to print, or they will have to make their own suitable alternative arrangements.

3.9 Any attempt to circumvent College procedures or any unauthorised attempt to access or manipulate College equipment or networks, may result in permanent disconnection from the wireless network, and any further disciplinary action as necessary.

3.10 All devices that need to access to power within the campus are required to be PAT tested in accordance with all College policies and regulations, please contact the estates department to have the device checked.

3.11 In the event that your device is lost or stolen or its security is compromised, you MUST promptly report this to the IT Support Unit (ext 222), in order that they can assist you to change the password to all College 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 the IT Support Unit in wiping the device remotely, even if such a wipe results in the loss of your own data, such as photos, contacts and music.

3.12 The College reserves the right to remotely wipe data from any device it has reasonable cause to believe holds College information in the event that the device is lost or stolen.