

**RNC Policy & Procedure: Bring Your Own Device (BYOD)**

|  |  |
| --- | --- |
| Responsibility:  | Technical Support Manager/Teacher in Charge - ICT  |
| Reviewed by:  | Technical Support Manager/Teacher in Charge - ICT  |
| Approved by SMT:  | December 2023 |
| Approved by Governor Committee:  | N/A |
| Date of next review:  | January 2025 |
| EIA Completed:  | 23/02/2017  |
| Published on Website:  |  Yes |
| Uploaded to Smartlog:  | No |
| Available to:  | RNC Students and Staff |
| Other relevant policies and reference documents - held on the RNC Intranet: [Policies, Procedures and Resources - Home (sharepoint.com)](https://rncac.sharepoint.com/sites/policiesproceduresresources/?locale=en-gb)* Acceptable Use Policy Computing and IT Systems and Resources
* E-safety
* Data Protection

  |
| **Commitment Statement** RNC is committed to the fundamental values of equality, diversity and inclusion, which creates a supportive environment for all members of our community to live, work and study. Our commitment to equality and diversity means that this policy has been screened in relation to the use of plain English, the promotion of the positive duty in relation to race, gender and disability and to eliminate discrimination to other equality groups related to age, sexual orientation, gender identity, marital or civil partnership status, pregnancy or maternity and religion or belief.  We believe that safeguarding has paramount importance and RNC recognises its responsibility and duties within the Government Prevent Strategy to be aware of and where appropriate act to ensure the safety of all students from radicalisation and extremism.  This document is available in alternative formats on request. If you think RNC can improve the fairness of this policy please contact the author who has responsibility for the review and update.    |

Contents

[1. Introduction 3](#_Toc152847441)

[2. Policy Scope 3](#_Toc152847442)

[3. Roles and Responsibilities 3](#_Toc152847443)

[4. Background 3](#_Toc152847444)

[5. Security 4](#_Toc152847445)

[6. Network Access 4](#_Toc152847446)

[7. Microsoft 365 5](#_Toc152847447)

[8. Data Access 5](#_Toc152847448)

[9. Printing 6](#_Toc152847449)

[10. Remote Access 6](#_Toc152847450)

[11. Support 6](#_Toc152847451)

[12. Personal Information and Data Protection 6](#_Toc152847452)

[13. Feedback and Further Information 6](#_Toc152847453)

**Bring your Own Devices (BYOD)**

#  Introduction

The Bring Your Own Device (BYOD) Policy is intended to provide a framework for the use by students and staff of their personal computer and mobile devices whilst connecting to or using information or technology resources belonging to RNC.

The policy complies with current legislation and current best practice regarding Cyber Essentials Plus Certification, Computer Misuse Act 1990, Data Protection Act 2018 (DPA 2018), United Kingdom General Data Protection Regulations (UK-GDPR), Prevent Duty, Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000 and applies to all computing and information technology facilities and resources within RNC specifically those accessing data, email, and internet.

# Policy Scope

The Policy applies to all users who have access to RNC IT systems, both on the premises and remotely.

Staff declaration will be agreed through Smartlog and Student declaration will be agreed by email.

The BYOD Policy applies to the use of all personal electronic communication devices such as laptop/desktop computers, tablets, mobile phones, games consoles, Braille note-takers and any mobile device that allows internet access.

# Roles and Responsibilities

Responsibility for the implementation of the BYOD Policy rests with the Executive Principal and Governors for ratification.

The day to day responsibility for BYOD Policy is delegated to the Technical Support Manager and the Teacher in Charge of Assistive and Digital Technologies.

# Background

In recent years personal mobile devices have become more capable and accessible to the point that many people wish to use them for day to day work and study.

RNC recognises that people have different ICT needs and preferences, including the ability to work from home or other accommodation, or because they find a particular device easier to use. To allow this, the use of personal devices is encouraged, subject to certain requirements which are detailed in this policy.

We also recognise the need for all students to have equality of opportunity and access to information, so have issued all students with laptops with their preferred assistive technology and additional braille technology if deemed appropriate at Pre-Entry assessment.  Students should use this equipment for all onsite and remote lessons. This is to ensure that the College are fully able to support them with their learning.

If students have personal devices and want to be supported with learning to use them, this can be arranged, it is expected that they will use college equipment during all lessons.

# Security

All personal devices connecting to the RNC network either on campus or remotely must have an up-to-date anti-virus solution installed (where applicable) and the latest security updates and patches installed. Personal devices must be protected by a password, PIN, pattern, biometric or other protection scheme. It is the user’s responsibility that their personal device is adequately protected, insured and kept safe whilst on campus and when working from home.

Staff and Students access to Microsoft 365 is protected with a 2-step verification process (also called multi-factor authentication). By setting up 2-step verification, you add an extra layer of security to your Microsoft 365 account. You sign in with your password (step 1) and a code sent to your phone (step 2).

Two-factor verification is more secure than just a password because it relies on two forms of authentication: something you know, and something you have with you. The something you know is your password. The something you have with you is a phone or device that you commonly have with you. Two-factor verification can help to stop malicious hackers from pretending to be you, because even if they have your password, odds are that they don't have your device, too.

RNC complies with Cyber Essentials Certification and the Prevent Duty. Security measures are in place to protect the user and RNC systems from accidental or malicious access, cyber security and inappropriate internet content. A Unified Threat Management (UTM) solution is installed between the RNC network and the internet, the UTM includes internet content filtering, packet filtering, firewall protection and logging of internet traffic.

Anti-virus and malware software is used to scan network traffic, computers, servers, internet and emails to prevent viruses, ransomware, malware and spam.

# Network Access

Most users will connect their own devices to the RNC network using the wireless networks. This extends across the campus and is the most convenient method for connecting. To minimise denial of service attacks and viruses infecting the core business data network, different wireless networks have been created on separate sub-networks.

RNC operates three main wireless networks:

* “RNC-CAMPUS” available to all students and staff
* “RNC-HALLS ” which is for student personal Wi-Fi devices that are unable to connect to RNC-CAMPUS or JANET (games consoles, streaming devices, Smart TV’s and speakers etc.)
* RNC-GUEST for stakeholders, general public and visitors.

Students and staff should only connect their college equipment to “RNC-CAMPUS”. Stakeholders, visitors and guests should only connect to “RNC-GUEST”.

RNC-CAMPUS and RNC-HALLS are protected using WPA2 encryption. A key will be issued to students and staff to allow access.

Except within certain rooms in the halls of residence, personal equipment should not be connected to the network using a cable. For example, users should NOT attempt to plug a laptop in to the wall in a teaching room, office or the Student Hub without prior consent from Technical Support.

Once connected to the network, users will be required to sign in periodically using their network login name and password. This is to ensure that all access is authorised and logged.

Internet activity is logged and can be traced back to the individual. This is a JANET acceptable use policy requirement (JANET are the academic internet service provider) and a requirement of the Prevent Duty. Users should also be aware that certain activities may be blocked, both in accordance with the Acceptable Use Policy, E-safety Policy and to control the use of internet bandwidth.

Guests accessing RNC-GUEST will be asked to provide an email address and a code will be sent to allow access and electronically accept the Acceptable Use Policy terms and conditions and privacy statement.

# Microsoft 365

RNC has a Microsoft 365 subscription which is available to all users whilst employed or attending RNC. This gives access to Online apps (Outlook, Word, Excel, PowerPoint, SharePoint, Teams etc.), cloud storage (OneDrive for work or school), mobile apps, productivity apps and permission to download and use the latest full version of Office on up to five devices.

# Data Access

Users can access email via Microsoft 365 Outlook Web Access (OWA) or through device Outlook client app, but whilst connected, devices must not be left unattended whilst email is open. RNC reserves the right to remote wipe the email on these devices if necessary.

Shared drives such as the X drive are not available on non-college devices and documents will need to be transferred using email, OneDrive for work or school or other technologies.

Cloud storage and messaging technologies such as OneDrive (personal), WhatsApp and Dropbox can be useful for users own private files and messaging but must not be used for any business owned, confidential or personal sensitive data. RNC users have access to 100GB (gigabyte) of cloud storage using OneDrive for work or school through their Microsoft 365 account.

Moodle VLE and Microsoft Teams is accessible everywhere and its use is encouraged for courses within learning.

# Printing

BYOD mobile printing is available. It works with Windows, macOS, Chromebooks, Android and Apple iOS operating systems. A small app is installed on your personal device so you will need administrator rights.

# Remote Access

VMware Horizon virtual desktop technology and Microsoft 365 Teams is available. Please contact Technical Support for more information.

# Support

RNC is aware that setting up and maintaining mobile devices can sometimes be a complex task. To help with this, Technical Support run a “laptop clinic” where any personal device may be brought along to a technician who will offer help, advice and assist in installing software.

IT support services offered by RNC to a user’s personal device is on a “no liability” basis and guarantee cannot be given to fix all problems. In some cases, personal equipment may have to be reset back to factory defaults or returned to the original vendor/manufacturer. It is the user’s responsibility to ensure that the device has correctly licenced software installed, anti-virus software, adequately backed up and the original installation media. If during a support session it is determined that any software installed on the personal device is not licenced correctly, the support session will be stopped.

If you ask a member of staff or a student to support you with your personal devices this is also “no liability", you are responsible for your own technology and should be careful to ensure that the person supporting has the skills and knowledge to fix the problem.

# Personal Information and Data Protection

This Policy should be read in conjunction with the Data Protection Policy. However, for the avoidance of doubt you may NOT store the following items on a personal device or send them via unencrypted email:

* Personal sensitive data which can be used to identify another person. For example, documents that contain just names would be fine (as names in themselves do not identify people), but documents that contain names and addresses would identify people and are not acceptable.
* Confidential college or personal material not relating to yourself

Virtual desktop and encryption systems exist that allow such data to be used outside of RNC where necessary. Confidential, personal or sensitive information must only be viewed in situations where the confidentiality of that information can be guaranteed.

# Feedback and Further Information

It is presumed that all students and staff will comply with the terms of these policies as part of the overall college policy, procedures and guidelines.

Any person found breaching the terms of the BYOD Policy may be prohibited from using personal devices and may also be subject to the college’s disciplinary procedures.

These policies will be reviewed regularly as circumstances dictate, by senior management staff who will also interpret the policies when required to do so. In all such matters, the final decision rests with the Executive Principal.

The college welcomes all constructive feedback on this and any other college policy. If you would like further information on BYOD or wish to send us your comments on our BYOD Policy, then please contact: Technical Support Manager or the Teacher in Charge of Assistive and Digital Technologies.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  | **Date**  | **Amendments**  | **Author**  |
| 1.0  | 30/05/18  | GDPR updates. Formatting  | AP  |
| 1.1  | 17/09/18  | Approved by SMT  | POK  |
| 1.2  | September 2019  | Date of review extended to Jan (from June 19) due to software updates scheduled for December 2019   | EG  |
| 1.3  | January 2022  | General updating and formatting. Updated Cyber Essentials to Cyber Essentials Plus Certification. Job title changed to Executive Principal. Office 365 changed to Microsoft 365. Section 4 updated to include student laptop and braille tech. Section 5 updated to include reference to MFA. Section 6 updated to included home Wi-Fi devices. Added new Section 7: Microsoft 365. Added new section 9: Printing. Added new section 10: Remote Access. Updated Section 11.  | AP/TA  |
| 1.4  | September 2023  | Section 6 updated Wi-Fi SSID’s.  Section 8 added WhatsApp.  Name change to Teacher in Charge of Assistive and Digital Technologies.    Updated Policy Front Page Moved version control Removed EIA   | AP/TA  |