

RNC Policy & Procedure: Acceptable Use Policy Computing and IT Systems and Resources

|  |  |
| --- | --- |
| Responsibility: | Technical Support Manager |
| Reviewed by: | Technical Support Manager/TiC IT Skills and Development BTEC/OCR |
| Approved by SMT: | March 2023 |
| Approved by Governor Committee: | N/A |
| Date of next review: | March 2025 |
| EIA Completed: | October 2016 & Reviewed May 2021 |
| Published on Website: | Yes |
| Uploaded to Smartlog: |  |
| Available to: | RNC Staff/Students/Volunteers |
| Other relevant policies and reference documents - held in the SharePoint Policy  Library: [RNC Policy Library](https://rncac.sharepoint.com/sites/policiesproceduresresources/Polices%20and%20Procedures%20Library/Forms/AllItems.aspx)   * Bring Your Own Device (BYOD) Policy * E-safety Policy * Data Protection Policy * Data retention and Disposal Policy * System Security Policy * CCTV Policy | |
| **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**

[RNC Policy & Procedure: Acceptable Use Policy Computing and IT Systems and Resources 1](#_Toc53313136)

[Acceptable Use Policy - Computing and IT Systems and Resources 3](#_Toc1951909581)

[1. Purpose 4](#_Toc2142210307)

[2. Network Access 4](#_Toc1827094322)

[3. Password Security 4](#_Toc1951880705)

[4. Hardware 5](#_Toc1772024094)

[5. Software 6](#_Toc1144790724)

[6. Email and Messaging 7](#_Toc1351052122)

[7. Internet 8](#_Toc2024722347)

[8. Filtering 10](#_Toc1718082433)

[9. Accessing RNC network remotely 10](#_Toc328920461)

[10. Network Drives 11](#_Toc271917347)

[11. Microsoft 365 11](#_Toc1603499057)

[12. Use of recording devices at RNC 12](#_Toc1290921453)

[13. Recording of evidence for couse work 12](#_Toc112501096)

[14. Use of photographs, images and videos at RNC 12](#_Toc1293597621)

[15. Photographs and video evidence for coursework 12](#_Toc610105314)

[16. Data Protection 13](#_Toc1865647369)

[17. General Notes 13](#_Toc627860799)

# Acceptable Use Policy - Computing and IT Systems and Resources

# Purpose

The Acceptable Use Policy (AUP) - Computing and IT Systems and Resources is intended to provide a framework for the use by students, staff and stakeholders of the computing and information technology resources of 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), 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 namely; network access, hardware, software, email and internet.

This Acceptable Use Policy is taken to include the JANET Acceptable Use Policy as published by Jisc.

# Network Access

All users of the computer network will be allocated a network login name on arrival at RNC. This provides access to the computer network and its associated resources. Users will also have a Microsoft 365 account that they will be encouraged to use, this will enable them to access their files through OneDrive and SharePoint cloud storage on multiple devices on and off campus.

# Password Security

As part of the initial sign-on procedure, users are required to supply a password with a minimum length of 12 characters. This provides security of access to individual drives and domain resources. Microsoft 365 user accounts will also have an additional layer of security for sign-ins by using multi-factor authentication (MFA) which uses both a password and an additional verification method such as a text message, phone call or smart phone app. The importance of password security cannot be over emphasised; therefore, users are expected to adhere to the following points:

Passwords must be kept private. They may not be revealed to anyone other than the Technical Support team to aid in fault finding or the Senior Management Team to access business critical data.

If a user thinks that their password has been compromised, they must change it immediately. Instructions on doing this can be obtained by contacting the Technical Support helpdesk.

Passwords should not be easy to guess, and users should avoid using names (such as pet names), common keyboard patterns and passwords they’ve used elsewhere. NCSC (National Cyber Security Centre) latest guidance recommends using three random words like 'coffeetrainfish' or ‘walltinshirt’.

If a user forgets their password, they can either reset it themselves by going to the self-passsword reset URL <https://passwordreset.microsoftonline.com/> or telephone the Technical Support helpdesk on 01432 376346 and the Technical Support team will reset their password.

In addition to password security, there are several general items that users should note:

* Users may not log into the computer network as any other user than themselves.
* Users must always sign out, restart or shutdown the computer from the start menu.
* Users must not leave computers unattended whilst they are logged in. Pressing the Windows Key and L together will securely lock a computer.
* Password Protected files are stored on the computer network at the owners risk. The central virus scanners cannot read these and may interpret them as viruses and delete them.
* Material which could be interpreted as illegal, inappropriate or in breach of licence conditions may not be stored on the computer network.

Important: Individual users can be held legally accountable for the contents of their drives, mail directories and any other files they store on the computer network and cloud. This means that users should take active steps to ensure their password is secure as outlined above.

Note:The use of RNC IT systems must be regarded as a privilege and not as a right. This privilege may be withdrawn if abused, or as part of a disciplinary procedure.

# Hardware

To maximise the potential of RNC’s computer system and IT resources, it is important to maintain control of the hardware in use.

RNC provides access to a range of both generalist and specialist hardware resources. However, freedom of access entails that users accept a general duty of care to take all proper precautions to prevent misuse.

Students are provided with a College laptop with their preferred assistive technology and they are to use this for **all** College work. These laptops are to be returned at the end of each academic year, for full maintenance checks and updating software. These will be returned to students in September. Maintenance checks will also be carried out throughout the year to ensure there are no problems. It is expected that students take their IT equipment home during all College holidays between September and July so they can access their work and classes remotely should this be necessary.

Staff may also be provided with a College laptop if it is thought to be necessary.

The use of the hardware resources provided must be regarded as a privilege and not as a right. This privilege may be withdrawn if abused, or as part of a disciplinary procedure.

To clarify the situation regarding potential misuse, the following guidelines outline restrictions on hardware resource usage:

* No items of hardware equipment may be abused in any way

All student laptops must be kept in the laptop bag provided by the College. Braille displays/Braille notetakers must be kept in the cases provided by the manufacturer.

* No items of hardware equipment may be used for purposes other than that for which they are designed
* Non portable items of hardware equipment may only be moved or relocated with the permission of a member of the Technical Support team
* Electrical/electronic equipment may not be disconnected without the authorisation of the Technical Support team.

Note: With due regard to the needs of other potential users:

* Any networked computer workstation may be used via a personal sign-in procedure
* Any general access multi-function printer or embosser may be used
* All general access specialist equipment may be used

# Software

To maximise the potential of RNC’s IT computer system, it is important to maintain control of the software in use.

General IT requirements will be accommodated using standardised hardware, software, and assistive technology. Software should be available on campus site licences. Standardisation and subsequent updating of the software provision will be the responsibility of the Technical Support team with consultation of staff.

RNC fully accepts the legal requirements in relation to IT and will not sanction the use of any illegally copied or acquired software.

RNC provides access to a range of both generalist and specialist software. However, freedom of network use entails that users accept a general duty of care to take all proper precautions to prevent misuse.

The use of the software provided must be regarded as a privilege and not as a right. This privilege may be withdrawn if abused, or as part of a disciplinary procedure.

To clarify the situation regarding potential misuse, the following guidelines outline restrictions on software usage:

* Existing software provided by RNC may not be uninstalled
* The configuration of any existing software provided by RNC may not be altered unnecessarily as this may lead to inaccessibility for the next user
* Software not authorised by the Technical Support team may not be installed on any networked computer or College-owned laptop.
* The download and installation of software from the internet may only be done with authorisation from the Technical Support team
* The use of games or similar software is prohibited on RNC’s core computer network and College-owned laptop computers.
* The installation of new, or the alteration of existing, device drivers is prohibited

Note: Any software available via the computer start menu or Microsoft Software Centre may be used within the constraints of individual licence agreements.

Installation of software not registered through RNC may be done by referral to, and at the discretion of, the Technical Support team. To enable proper support and security the master copy must be held by the Technical Support team. Installation of some software may be denied for security or other reasons or may only be permitted on non-networked computers.

# Email and Messaging

Electronic mail (email) and messaging includes all electronically transmitted messaging systems including but not limited to Microsoft Teams Chat, Zoom Chat, WhatsApp and SMS. RNC provides access to a registered email system. However, freedom of network use entails that users accept a general duty of care to take all proper precautions to prevent misuse. Email and messaging must be used in a professional and courteous manner and not to be used to bring RNC into disrepute.

Misuse of RNC systems may have serious implications. Use must be regarded as a privilege and not as a right. This privilege may be withdrawn if abused, or as part of a disciplinary procedure.

To clarify the situation regarding potential misuse, the following guidelines outline restrictions on email usage.

Email and messaging must not be used:

* Within lectures or tutorials unless specifically authorised by a member of staff
* To transmit or receive discriminatory, threatening, harassing, bullying, sexually inappropriate, offensive or other illegal or improper messages
* To download unauthorised software
* For the purpose of bulk messaging unless authorised by a member of the Technical Support team
* To instigate, propagate or participate in the transmission of ‘chain letter’ mail
* Messaging systems (WhatsApp etc.) should not be used to transmit and discuss personal sensitive data

Note:

* Emails received from unknown sources should be treated with caution especially with the increase in phishing scams and viruses being spread via email, and deleted before opening
* Email should not be thought of as “private”, it can be intercepted and read easily, either by design or by accident
* DPA 2018 requires that personal sensitive data included in emails must be encrypted and deleted as soon as no longer required
* File attachments should only be sent when absolutely required; often in the case of internal messages it is possible to state the location of a file on a shared drive
* External email services (e.g. Outlook, Hotmail, Gmail) may be used subject to these conditions as well as any conditions imposed by the provider
* Staff who leave the organisation will have their email account suspended in its current state and will not be able to access it. After six months, it (and all the contents) will be permanently deleted. For this reason, team-based users are encouraged not to use personal email addresses but to ask technical support for a shared mailbox with a generic name (e.g. "tech", "sales" or "kitchen").
* "Deleted Items" will be kept for a short time only, after which they will be permanently removed. "Deleted Items" should be treated like a bin that can be emptied at any time and should never be used for filing messages.

# Internet

This covers all internet services including but not limited to the World Wide Web, email, cloud storage and services, social media, video conferencing, communication applications and mobile applications etc. The aim of RNC in offering access to the internet is to further educational goals, for business research, and to aid continuous professional development. Using the internet enables students and staff to access a wide range of information services and exchange messages with other internet users. However, freedom of network use entails that users accept a general duty of care to take all proper precautions to prevent misuse.

Use must be regarded as a privilege and not as a right. This privilege may be withdrawn if abused, or as part of a disciplinary procedure. Misuse may result in user internet access being limited or disabled.

Abuse of RNC websites may have serious implications for other sites and have financial and reputational implications for RNC.

RNC has a contractual duty as part of its agreement to connect to the JANET internet network to abide by their Acceptable Use Policy (AUP). This includes the ability to track and report suspicious internet traffic, virus infection or abuse and a legal requirement to be able to provide logs to law enforcement agencies.

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. All user internet traffic is monitored, filtered and logged. Should users access inappropriate content (as defined in the Prevent Duty) and this is detected, alerts and logs are generated and checked by the Safeguarding Team.

To clarify the situation regarding potential misuse, the following guidelines outline restrictions on internet access.

The Internet must not be used for any of the following:

* Accessing inappropriate content as defined under the Prevent Duty
* Intrusion of privacy or theft of intellectual property which causes breaches of confidentiality and/or copyright
* Creation or transmission of any offensive, discriminatory, threatening, seditious, illegal, obscene or indecent images, data or material.
* Viewing, downloading, storing or printing of any offensive, discriminatory, threatening, seditious, illegal, obscene or indecent images, data or material
* Viewing or downloading unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others
* Bringing RNC into disrepute
* Dissemination of unsolicited and unwanted, and possibly offensive and/or illegal material
* Destruction of information and/or temporary disabling of remote systems
* The subscription to any services not authorised by RNC
* The abuse of any Chat facility
* The transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks: e.g. the sending of junk mail or other advertising material over the Web
* Creation or transmission of material which contravenes RNC’s Equality, Diversity and Inclusion Policy or which is discriminatory against individuals or groups
* Deliberate unauthorised access to facilities or services accessible via the internet: e.g. attempting to access systems and files by “hacking”

There may be permission granted for material included in the above definitions to be used for research purposes. This permission will only be granted when approved by the Lead Designated Safeguarding Officer. Students should only access such material when in a classroom situation where they can have direct support and monitoring from a member of staff.

Note: Where the Internet is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the internet.

# Filtering

RNC subscribes to a “blocking service” that aims to identify inappropriate content to prevent users from accidently accessing offensive or otherwise inappropriate content. Whilst RNC has taken reasonable action to prevent access to inappropriate content it should be noted that no such system is perfect and will on occasion both allow access to inappropriate material and block access to legitimate material. If a user accidentally accesses inappropriate material, they should inform Technical Support so a block can be manually introduced. If a user requests a website to be unblocked this will only be done in the case of a clear business need and only then when authorised by the Safeguarding team or Technical Support Manager.

Some websites such as some media streaming providers and online gaming sites are blocked both due to content reasons and due to excessive bandwidth requirements. Technical Support staff are responsible for the correct operation and monitoring of the filtering and blocking systems.

# Accessing RNC network remotely

Access to the network from outside of RNC is available to all users. Access to services is via a secure web portal either through VMware Horizon or Microsoft 365 with the exception of the Virtual Learning Environment which is available on a separate web address. Guidance on how to access these systems will be provided on request by the Technical Support team**.**

Staff who access the College systems from the internet must use a device that is:

* Fully patched with all the latest operating system security updates
* Running up to date and approved security software such as firewall/anti-virus and anti-malware applications
* Using a modern operating system and internet browser
* Adhering to the RNC “Bring Your Own Device” (BOYD) policy

For further information please contact the Technical Support helpdesk.

# Network Drives

Staff may be given access to several network drives (also known as file shares). These drives (if allocated) must be used for the following purposes:

* P - contains various databases that staff may access. Files may not be written here
* W - contains various network software. Files may not be written here
* X - a shared repository of files for staff. The X drive is organised by department and team, is access-secured for each team and all work-related files must be stored here
* Y and Z - contain users personal network profiles and should not be accessed or modified in any way

These network drives are backed up by the Technical Support team. It is not necessary for users to make their own backups.

Locations not listed above, including the desktop, may be deleted without warning and are not backed up.

# Microsoft 365

Students and staff have access to Microsoft 365 cloud services which includes cloud storage (OneDrive), collaboration and communication tools (Teams and SharePoint etc.) and Office applications (Word, Excel, Outlook etc.). These cloud services can be accessed using network sign-in details from an internet browser (Microsoft recommends using Edge Chromium or Google Chrome), or from a desktop application.

Data stored in the cloud is at the risk of the owner and is not backed up by RNC. To allow users the ability to restore files themselves, Microsoft has built a Recycle Bin into OneDrive and Teams. Files that are deleted from OneDrive or Teams reside here for 90 days and can be restored by the user at any point during that 90-day period; after this period, they are automatically deleted.

Guidance on how to access these systems will be provided on request by the Technical Support team.

# Use of recording devices at RNC

RNC understands how useful recording devices can be for note taking but must ensure that these devices are not misused. Although it is not illegal to use a voice recorder to record someone without permission, it is illegal to share the recording or edit it. It is RNCs policy that permission must be confirmed before recording. If the recording is to be shared with others, it is the responsibility of the individual making the recording, to obtain permission from those involved in the recording. Recordings must not be uploaded to social media channels or shared using email or file sharing facilities without written consent.

# Recording of evidence for couse work

Many qualifications allow recordings to be used as evidence. When this is needed the student must always be made aware that they are being recorded and that the recording may be asked for by the exam board.

# Use of photographs, images and videos at RNC

RNC understands that photographs, images and videos are used to market the College and to create memories of special moments. The College does not want these to be misused. Therefore the College policy is that permission must be confirmed before taking photographs, videos or using images.

Photographs or videos must not be taken without permission of those within the photograph or video. Separate permission must be confirmed before posting and/or sharing photographs, videos or images. Those sharing photographs, images and videos must ensure that these cannot be re-shared or edited.

Only official RNC social media accounts are to be used to share photographs, images and videos. Social media settings must be kept private so that others cannot share or edit posts.

Consent permissions are received by residential staff at either NSC or when the student starts at college, and the information is shared with Marketing and Communications. Hard copies are kept in student files in halls, and students/parents of u18s can retract consent at any given time if they feel the need to

# Photographs and video evidence for coursework

Many qualifications allow for such evidence to be used. When this is needed the student must always be aware that they are being videoed or photographed and that this evidence may be asked for by the exam board.

# Data Protection

People who access data which can personally identify living people have several obligations under the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). Failure to adhere to these can not only lead to disciplinary action but can also render the person open to prosecution. Further information can be found in the Data Protection Policy.

Personal identifiable data may **only** be stored on the X: drive and MIS systems, in authorised areas. These areas are security protected to avoid unauthorised access.

If a user needs to work on personal information remotely, they must use the VMware Horizon system which is a secure encrypted remote desktop solution that never allows the data to leave RNC. The user must take steps to ensure that only authorised staff can see the information on the screen.

Printing of personal data is discouraged. However, sometimes it is necessary. If such data must be printed, the user is responsible for ensuring that it is collected from the printer immediately and not left unsecured anywhere. RNC operates a "clean-desk" policy with regards to personal data, paperwork most not be left unattended and must be locked away when not in use.

Printed personal data must be disposed of securely using a cross-cut shredder. Facilities for this are provided around the campus. Under no circumstances may it be put in the general or recycling waste.

If there is a requirement to send or access personal identifiable data off-site, it must be done in a secure manner. If this is by email or removable media, it must be encrypted. Please contact Technical Support for further information.

# 17. General Notes

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

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

Any person found breaching the terms of the Acceptable Use Policy will be prohibited from using the computer network and IT systems and may be subject to RNC’s disciplinary procedures.

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Amendments** | **Author** |
| 1.0 | 23/05/18  09/07/2018 | Formatting. ‘College’ changed to RNC. Data Protection Action changed to ‘Legislation’. Principal changed to ‘College Principal/Charity Chief Executive.  GDPR updates. General updating – changes tracked. EIA added.  SMT approved | EG |
| 1.1 | September 2018 | General updating. EIA added. | POK |
| 1.2 | June 2019 | Policy reviewed no changes required | POK/AP |
| 1.3 | November 2020 | General updating. Job title changed to Executive Principal. Section 2 updated to include reference to student college laptops. Section 4 Email updated to include messaging systems. Added new Section 9: Microsoft 365. | AP/TA |
| 1.4 | January 2022 | General Updating. Cyber Essentials updated to Plus. Section 4 updated student college laptops. Section 6 included WhatsApp. Section 10 removed defunct file shares and drives. Removed declaration forms as now done electronically. | AP/TA |
| 1.5 | February 2023 | Section 3 Password Security updated to latest NCSC guidance. General updates. | AP |
| 1.6 | September 2023 | Interim update to include new sections 12-15:   * Recording of evidence for course work * Use of recording devices at RNC * Use of photographs, images and videos * Photographs and video evidence for coursework |  |