Royal Northern College of Music
IT Policy
Policy & Procedure
Department: IT
Document owner: HIT
Approval Committee: Executive Committee
Revised: February 2025
Period of Approval: 3 years
Review Date: February 2028

1. Purpose

The purpose of this document is to inform users of the regulations around acceptable use of RNCM IT facilities, for the benefit of the RNCM and all users.

2. Scope

This policy applies to employees, students, contractors, consultants and temporary staff, including casuals and work-experience staff at the RNCM, and including all personnel affiliated with third parties and College partner organisations (defined as 'users').

The policy applies to IT and communications equipment that are owned, leased or managed by the RNCM; any equipment attached to College systems; use of any RNCM provided accounts (e.g. RNCM email addresses or eduroam accounts); any third party services used by the RNCM; and conduct on any RNCM websites, including RNCM managed pages, e.g. RNCM social media pages (collectively defined as 'RNCM systems').

3. Roles and responsibilities

All users are required to familiarise themselves with these policies and to work in accordance with their guidelines. This document is available on the Intranet/Moodle. Users should note that depending on severity, breaches of this policy could lead to disciplinary proceedings, and could constitute gross misconduct.

It is a condition of employment that all employees abide by the College's regulations and policies. Any employee found to have violated these policies may be subject to disciplinary action, in line with the College's Disciplinary Policy. A breach of the College's IT security may be regarded as gross misconduct and will be considered as potential grounds for dismissal.

Students will be subject to disciplinary action under the Student Conduct and Discipline Policy.

Users are required to familiarise themselves with requirements under the Counter-Terrorism and Security Act 2015, requirements in relation to the College's Information Security Policy, and by implication, with the GDPR.

Staff are required to maintain a basic level of proficiency in the technology relevant to their job role. For occasional users, this will include an awareness of how to stay safe online and keep RNCM data secure (avoiding phishing emails etc). For staff who use a computer as a part of their work, this will also include maintaining competency in software relevant to their role.
Cyber security training is provided to all staff, either as either optional (but highly recommended), or mandatory, depending on the role.

4. Acceptable use

The use of RNCM systems is subject to all applicable College policies eg Dignity at Work, Belonging Equity Diversity Inclusion Policy etc; the JISC Acceptable Use Policy (currently available at https://community.jisc.ac.uk/library/acceptable-use-policy); and relevant law.

The RNCM reserves the right to audit networks, systems and devices to ensure compliance with this policy. Users must not perform any act, whilst using College computing facilities,

which would bring the College into disrepute, or circulate any information of a kind which is unlawful, prohibited or likely to undermine the College's reputation.

The RNCM has a statutory duty to have due regard to prevent people being drawn into terrorism. IT resources and facilities must not be used in such a way that would breach this or any other terrorism related legislation, and access to material that promotes terrorism is not permitted without a specific research exemption.

The following activities are prohibited:

General Conduct

- The creation, download, storage, usage, dissemination or display of any material that is offensive, indecent or illegal, including material of a discriminatory, defamatory, extremist, or terrorist nature.
- Engaging in any threatening, bullying, abusive, discriminatory or defamatory behaviour.
- Unauthorised copying, including downloading from/uploading to the internet, of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the RNCM does not have an active licence.

Legal

- Providing information about, or lists of, the RNCM staff or students to parties outside the RNCM, except where this is done under a data sharing agreement or otherwise in compliance with the College's Information Security Policy, and by implication, with the GDPR. The installation of any software that is not correctly licensed.
- Any other unlawful activity.

Actions affecting the services

- Using shared services in any way that has an undue impact on other users, for example using excessive amounts of disk space or network bandwidth.
- Scanning or otherwise analysing the systems to attempt to discover security weaknesses, without express permission from the Head of IT or IT Infrastructure Engineer.
- Any action that unduly interferes with the running/provision of the services; for instance, anything constituting a DoS attack, deliberately installing malicious software, or hacking.
- Interfering with RNCM systems without good reason. This includes disconnecting/moving equipment, connecting unapproved equipment, unauthorised access or modification of data, or setting up wireless networks on college property (other than personal use networks), or allowing a third-party to perform any of the above.

Work related

- The purchase, setup or installation of, or subscription to any new IT system or equipment without prior consultation with the IT department.
- Purporting to officially represent the RNCM via the services, except as a legitimate part of a user's work.

- Users may not set up unauthorised web sites on RNCM computing facilities (authorisation is provided by the Head of IT and the Director of Marketing and Student Recruitment); publish pages on external web sites containing information relating to the RNCM; enter into unauthorised agreements on behalf of the RNCM via a network or electronic communication system.
- Any other activity which could bring the RNCM into disrepute.

5. Conduct

Communication online, through email and via social media sites and tools must protect the RNCM's institutional voice by remaining professional in tone and in good taste. Staff/students of the RNCM who use online communications must not give the impression that their communication represents the explicit position of the RNCM without authorisation from the Marketing and Student Recruitment Department.

Staff/Students should be aware of their conduct online, especially on social media and through email, and the potential this has to cause distress, annoyance or needless anxiety to other individuals.

Where it is possible to link an individual's online identity to the RNCM (eg talking about the RNCM, mentioning studying or working at the RNCM, using an RNCM email account), then that user should be mindful that they could be considered to be representing the RNCM. In this situation, users are expected to behave in ways consistent with the RNCM's policies and values.

Further information can be found in the RNCM Email Good Practice Guide and Social Media protocol.

The RNCM IT facilities are provided primarily to be used for College purposes, and users should be aware that the RNCM can make no guarantees of privacy when using college services. The RNCM may employ web filtering technologies. RNCM IT accounts, including email accounts may need to be accessed by authorised personnel in the event of unexpected absence, or to comply with legal requirements imposed upon the College.

Use of College computing facilities should be for work purposes. Limited personal use of email and the Internet is acceptable as long as it does not affect the performance of the post holder or the performance of College IT systems. Private work use is not permitted if it is for personal gain.

6. Information Security

Individuals must, at all times, act in a responsible and professional way and must refrain from any activity that may jeopardise security. Users will be assigned with usernames and passwords for RNCM systems. It is the responsibility of users to keep these passwords secret and secure, and to let the IT department know immediately if they have reason to suspect somebody else may know their passwords (for instance if a user has fallen victim to a phishing attack). Users are responsible for any conduct that occurs through use of their username/password.

Users must be mindful of the reputational and legal risks of any data loss, and take all sensible precautions to avoid such loss. Typically this would involve storing data/documents only on College servers or College OneDrive/SharePoint and taking reasonable precautions to ensure any computer they use to access College data (e.g. home computers, internet cafes) is secure.

Users must comply with the Information Security policy, and all relevant related policies. Additionally, users must adhere to the following guidance:

- Security - electronic: All data should be managed securely, and access only given to those with a legitimate requirement. Users are responsible for the security of the data they are working with. Mandatory formal cyber security training is provided to users with access to critical data. Users with only limited access to College data are provided with an informal training course. While this is not mandatory, it is highly recommended.
  Users should ensure that no unauthorised person can access computers which are left logged on and unattended.
  Computers left unattended for a short time in a safe location (eg an office) should be locked (Windows+L on a PC, Control+Command+Q on a Mac). Computers unattended for a longer period of time should be shut down.
  Memory sticks should not be used except for public data. Instead, files should be transferred using OneDrive/SharePoint.
  Payment card data (e.g. 16 digit credit card numbers, CSC/CVCs etc) must not be written down, stored on any College system, or transmitted via any text-based messaging system.

- Bring your own device (BYOD): Where possible, users should work on College devices, especially when working with sensitive data. If a non-College computer is used to create or access sensitive information, users must ensure that the computer has all relevant security updates, has functioning, up-to-date anti-virus software running, and that no-one else can use it to view College information. College data must not be permanently stored on non-College computers. The easiest way of achieving this is by working on documents live via Microsoft 365, instead of downloading copies.

- Security - paper: All paper records containing personal information, e.g. student or staff files, must be stored in lockable cabinets, cupboards or drawers. This storage furniture should not be left unlocked if an office or other room is left unattended for a period of time and could be accessed by others who do not have permission to view the information. No personal data should be left accessible on desks overnight. Save in very exceptional circumstances highly confidential paper documents should not be taken outside the College; if this is necessary they should be stored securely (locked cabinet, secure briefcase kept with the user) at all times.
  Secure paper disposal bins must be used to dispose of all paper records once they are no longer required.

- Data sharing: Sensitive information may be shared only where the conduct of College business requires this, where it is allowed within the law or where the data subject has given specific consent.
  When emailing sensitive information to other members of the College, always use the College email address, not a personal one. Ensure the correct address is used before sending the email.
  The sending of attachments with confidential data is discouraged; instead users should share a link to files within OneDrive/SharePoint. This enables links to be revoked if an email is sent to the wrong person, and allows editing of shared documents after the email has been sent.

- Web services: Unapproved third party web services, e.g. Dropbox, must not be used for storing, processing and transferring data which is (a) sensitive [defined in

Information Security Policy appendix 1]; (b) of such criticality that functions or operations would be disrupted should it be lost or become unavailable or corrupted [see Business Continuity Plans]; or (c) market sensitive information [as agreed by the Director of Finance]. Personal data must be stored only on servers hosted in EU, or using a supplier whose services comply with the EU-U.S. Privacy Shield Framework2 and thus with the GDPR.

Additional guidance on working securely can be sought from the IT department.

7. Exceptions

Exceptions to this policy may be made in some circumstances, e.g. legitimate research needs. Exemptions should be sought from the Head of IT.

8. Related documents

- Social Media Policy – Staff
- Social Media Policy – Students
- Information Security Policy

ROYAL NORTHERN COLLEGE OF MUSIC

POLICY APPROVAL/REVIEW PROCESS

Release: Final
Author: Deborah Harry
Document Number: 2

AMENDMENTS SINCE DRAFT

ISSUE No	PAGE	DETAILS	DATE	ISSUED BY
1		First draft	February 2025	Deborah Harry
2		Final – ready for publication	February 2025	Deborah Harry

Approvals

This document requires the following approvals.

Name/Committee	Date	Version
Executive Committee	18 February 2025	1