Royal Northern College of Music

IT Policy

Policy & Procedure

Department: IT

Document owner: HIT

Approval Committee: Executive Committee

Revised: February 2018

Period of Approval: 3 years

Review Date: February 2021

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 at the RNCM, 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 (eg RNCM email addresses or eduroam accounts); any third party services used by the RNCM; and conduct on any RNCM websites, including RNCM managed pages, eg 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 potentially 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 Data Protection Policy, and by implication, with the Data Protection Act.

4. Acceptable use

The use of RNCM systems is subject to all applicable College policies eg Dignity at Work, Equality and Diversity 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 on a periodic basis 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 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.

- Unauthorized 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 Data Protection Policy, and by implication, with the Data Protection Act 1998.
- 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.
- 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).

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 Head of Marketing and Communications); 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. <u>Conduct</u>

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 positioning of the RNCM without authorisation from the Marketing and Communications 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. RNCM IT accounts, including email accounts may need to be accessed by authorised personnel in the event of unexpected absence, or to comply with the 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 might involve storing data/documents on College servers, or on encrypted memory sticks, 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: Assess the sensitivity of all information created and received; and take proportionate measures to ensure that data are held securely (including access to the website). This includes appropriate use of passwords, PIN, encryption, etc. when using portable or fixed devices, whether owned by the College or not. Users should ensure that no unauthorised person can access computers which are left logged on and unattended.
  Sensitive data must only be stored on College-owned fixed or portable devices that are encrypted, e.g. encrypted laptops and memory sticks.
- Bring your own device (BYOD): If a non-College computer is used to create or access sensitive information, users must ensure that the computer has up-to-date security protection, and that no-one else can use it to view College information. Data must transferred securely to a College-owned device and any data held on the non-College device must be deleted after use (including removal from any temporary or trash files).
- 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.

- 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 e-mailing sensitive information to other members of the College, always use the College e-mail address, not a personal one. Ensure the correct address is used before sending the e-mail.
- Remote access: When off campus (i.e. using remote access) to access College e-mail or data, either use links provided via the College website, intranet and Moodle or, if mobile devices are used for this purpose, make sure they are password or PIN protected, or otherwise encrypted. Do not set up passwords which are then automatically remembered by the device for future use if on a non-College owned machine (e.g. home device, internet café, open Wi-Fi, etc.).
- 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 and Strategic Planning]. 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.
- Safe disposal: Use shredding machines or College-approved shredding services for disposal of classified paper documents. Any unwanted, damaged or obsolete computer hardware must be disposed of through the IT Department.

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

7. Exceptions

Exceptions to this policy may be made in some circumstances, eg 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