ROYAL COLLEGE OF MUSIC

IT POLICIES

2018-19

This document contains important information on the policies in force for any users of the RCM network and RCM Technology. All users are required to familiarise themselves with this document and the Acceptable Use Policy (AUP).

Version History	Review Date	Teams
V 1.0	10/10/2007	NW
V 1.1	1/11/2007	NW
V 1.2	19/11/2008	NW
V 1.3	29/1/2010	NW
V 1.7	16/09/2014	MS
V 1.9	8/07/2016	MS
V 1.10	20/09/2017	MS
V 1.11	22/09/2017	MS
V 1.12	15/05/2019	BP

1. Introduction and Overview

1.1 Scope of IT Policies

This policy applies to employees, students, contractors, consultants and temporary staff at the Royal College of Music, including all personnel affiliated with third parties. These people are referred to as 'users' for the purpose of this document. This policy applies to all equipment that is owned or leased by the Royal College of Music and any equipment attached to the Colleges systems with the agreement of the RCM Technology.

1.2 Purpose

The purpose of this document is to outline the policies applicable to the use of the Royal College of Music's IT and network systems. All users of the Royal College of Music's IT systems will be bound by these policies and they should ensure they are fully aware of their obligations, as set out in this document.

1.3 Disciplinary Procedures and Enforcement

All users authorised to access the College network to use RCM systems and facilities are required to familiarise themselves with these policies and to work in accordance with their guidelines. All new members of staff will be directed to this Policy document from the HR Manager and similarly all new students will be directed to this Policy on registration, where further information can be supplied on request.

Existing staff and students of the College, authorised third parties and contractors given access to the College network will be advised of the existence of this policy statement and the availability of the associated policies, codes of practice and guidelines which are published on the College Intranet.

Any member of staff or visitor found to have violated these policies will be subject to disciplinary action, in line with the College's Disciplinary Procedures. A flagrant 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 Code of Conduct.

Although these policies are not part of any formal College employment contract, it is a condition of employment that all employees will abide by the College's regulations and policies.

In certain circumstances, legal action may be taken. Failure of a contractor to comply could lead to the cancellation of a contract.

2. Policies

2.1 IT Security Policy

2.2 Introduction
This policy complies with the JISC, JANET Security Policy. In respect of the RCM this duty includes:

- Establishing policy rules
- Encouraging users to act responsibly and ensuring that they are enabled to do so
- Exercising responsibility in providing access to JANET
- Taking measures to protect against attack
- Providing adequate disciplinary and other procedures to enforce an appropriate local policy
- Assisting in the investigation of a breach of security

2.2.1 Purpose

Any breach of security of an information system could lead to loss of security of personal information. This would be an infringement of the Data Protection Act 1998 and could lead to civil or criminal proceedings. It is vital, therefore, that users of the College's information systems comply, not only with this policy, but also with the College's data protection guidance, details of which may be found on the College Intranet.

With an increasing reliance on electronic information at the RCM comes a corresponding concern for the security of that information. This IT security policy aims to maintain availability and confidentiality while guaranteeing the continued integrity of this information, by the provision of adequate security measures.

The RCM aims to achieve effective security by maintaining compliance with relevant legislation, and guidance from JISC and others.

A continual review process of the soundness, adequacy and application of physical security, software security and other controls, will ensure that the College's evolving needs in the area of IT security are adequately met.

The College wishes to promote effective and efficient IT security controls at reasonable cost.

This security policy provides a framework within which to define roles and responsibilities with respect to data security, and makes explicit the RCM's attitude to any actions which threaten the security of its information assets.

2.2.2 Policy

The policy encompasses all elements identified within the JISC, JANET Security Policy.

Physical Security

- RCM Technology will provide a secure, climate-controlled machine room with suitable power supply provision to enable centralised computing facilities to the College.

- RCM Technology will take reasonable steps, e.g. via Kensington locks, to secure computers owned by the College located outside on the machine room.

- RCM Technology will ensure that physical security measures are in line with the College's insurance policy.

Anti-Virus Software

- Every computer owned or managed by the College or connected to the College's IT systems must be constantly running up to date anti-virus software.

- Computers not meeting this requirement will be barred from accessing the College's networks until rectified, exceptions may be required by approval from the technology and deputy technology manager.

IT Security Reviews and Penetration Testing

- RCM Technology will undertake periodic security reviews, which may involve monitoring and auditing computers owned by the College.

- Network penetration tests will be carried on an annual basis as a minimum and may be required more frequently should significant changes be made to the College's IT systems.

- Network penetration tests must be carried out by an independent 3rd party.

Computer Access

- Access to the College's IT Systems will be provided via User Accounts.

- User Accounts will only be issued to **real** individuals with the authority of the relevant departmental manager or professor. Technical system accounts will first be approved first by the Head of RCM Technology.

- RCM Technology upon graduation, will give student user accounts restricted access until 31st October.
- RCM Technology will set user accounts for staff to automatically be disabled and accounts will be removed 60 days after contract finish date provided by Human Resources. Extensions to this will only be provided for a maximum of 6 months for data protection purposes and on the written authorisation of the Head of HR and the RCM Technology Manager.

- User Accounts are provided subject to the College's IT Policies, breach of these policies by an individual will result in access rights being revoked.

Configuration Management

- Only RCM Digital personnel are permitted to purchase, install and delete software on computers owned by the College.

- Only RCM Digital personnel are permitted to configure system level settings and delete software on computers owned by the College.

- Staff and students are permitted to configure options for their desktop\laptop applications such as Word and Excel, on computers owned by the College. This does not include the installation of Microsoft Office add-ins.

- Staff and students issued with RCM laptops are required to connect to the network regularly to ensure software updates are applied.

- RCM Technology will conduct a risk assessment of any change to the RCM IT Systems in order to understand the IT security risks associated. RCM Technology reserves the right to prevent any change to IT Systems they feel compromises IT Security or take other appropriate action to remedy security risks presented by requested changes.

2.2.3 Roles of Responsibilities

All College Staff and Students are responsible for promoting awareness of IT security and observing and adhering to this policy.

All College Staff and Students are responsible for reporting any theft of personal or RCM computing equipment to RCM Technology as soon as possible.

The Technology Manager is responsible for approving IT Security policy and for ensuring that it is implemented.

RCM Technology are required to implement these policies and are responsible for ensuring that staff, students and other persons authorised to use those systems are aware of and comply with them and the associated codes of Practice.

RCM Technology are responsible for advising the Directorate group on the appropriateness of and the College's compliance with this policy and its associated codes of practice.

The Technology Manager is responsible for the promotion of this policy throughout the College, analysis of the annual assessments of security and the reporting of these to RCM Directorate and maintaining records of misuse of the College systems.

The Technology Manger is responsible for ensuring the regular review, updating and re-issue of the security policy, associated codes of practice and any relevant guidelines.

The Deputy Technology Manager is responsible for the management of the desktop infrastructure and the provision of support and advice to RCM staff and students.

The RCM's Managed Service Provider, reporting to the Deputy Technology Manager, is responsible for the pro-active management of the College's Network and Server devices.

The Technology Manager is responsible for ensuring annual Penetration Testing is conducted and remedial actions are carried out in a timely fashion.

It is the responsibility of each user to ensure his/her understanding of and compliance with this Policy and the associated Codes of Practice.

2.2.4 Data and Security Breach Reporting

RCM Technology will monitor network activity reports from JISC and other security agencies and take action/make recommendations consistent with maintaining the security of College systems and data.

Users suspecting that there has been, or is likely to be, a breach of security must inform the RCM Technology Helpdesk immediately who will follow the current Data Breach Policy and advise the Incident Management Team on what action should be taken.

Users must inform the RCM Technology Helpdesk immediately of any suspected virus.

In the event of a suspected or actual breach of security, the Technology Manager may, after consultation with relevant departmental managers, make inaccessible/remove any unsafe user/login names, data and/or programs on the system from the network.

The Technology Manager (and in his/her absence other members of the Data Breach Incident Team) have the authority to take whatever action is deemed necessary to protect the College against breaches of security.

2.3 Password Policy

2.3.1 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Royal College of Music's entire corporate network. As such, everyone issued with a user account is responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.3.2 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2.3.3 Policy

- Users are responsible for the security of their passwords and accounts.

- All active system-level passwords must be part of the Technology Department-administered global password management database.

- Remote Access to the Royal College of Music networks will be controlled using a VPN network and/or a Remote Gateway connected to a dedicated terminal server.

- RCM Technology enforce the following User Account password rules for all staff except **part-time professors:**

    o All passwords must be changed on at least a quarterly basis
    o The password must contain no less than nine characters
    o The password must contain characters from three of the following four categories:
        ▪ Latin uppercase letters (A-Z)
        ▪ Latin lowercase letters (a-z)
        ▪ Numbers (0-9)

- Special characters e.g.!@$%^

- It is the responsibility of the individual to ensure that they conform to the rules described below:
  o Do not use any of the examples as passwords in this document
  o The password must not contain common usage words such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "the Royal College of Music", "RCM", or any derivation.
    - Composers names, music titles or any other musical terms
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, 123321, etc.)
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1)
  o The password should not be a word found in a dictionary (English or foreign)
  o Do not write usernames or passwords down or store them in a file on a computer
  o Passwords must not be the same as usernames
  o Do not use the same password for Royal College of Music accounts as for other non-Royal College of Music access (e.g., personal ISP account, option trading, benefits, etc.)
  o Where possible, don't use the same password for various Royal College of Music access needs.
  o Do not share the Royal College of Music usernames or passwords with anyone.
  o Don't reveal a usernames or password in an email message
  o Do not use the "Remember Password" feature of applications (e.g. Outlook, Internet Explorer etc.)
  o If you suspect an account or password has been compromised, report the incident RCM Technology and change all passwords.
- For part-time professors, all of the above applies with the following exception:
  o Password are valid for one year, not 90 days.
  o Passwords are nine, not eight, characters.
  o More than just upper and lower.
  o Students and staff are required to enrol with the RCM Password Portal Service.

2.4 Acceptable Use Policy

2.4.1 Overview

The College's aim in this Acceptable Use Policy is to reflect the Royal College of Music's established culture of openness, trust and integrity. The AUP is intended to protect the staff, students and the College as a whole from illegal or damaging actions by individuals, either knowingly or unknowingly.

2.4.2 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and network access at the RCM. These rules are in place to protect the employees, students and the RCM. Inappropriate use exposes the College to risks including virus attacks, compromise of network systems and services, and legal issues.

2.4.3 General Use and Ownership

While the RCM Technology aims to provide a reasonable level of privacy, users should be aware that the data they create on the College systems remains the property of the Royal College of Music. Data saved MAY be seen by other RCM users and should not be regarded as personal.

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 your job or the performance of other College IT Services. Members of staff and students are responsible for exercising good judgment regarding the reasonableness of personal use.

For security and maintenance purposes, authorised individuals within the Royal College of Music may monitor equipment, systems and network traffic at any time, as per the Auditing & Monitoring Policy. Members of RCM Technology abide by the JANET-CERT Draft Charter for System and Network Administrators, which can be found here:

https://community.jisc.ac.uk/library/janet-services-documentation/suggested-charter-system-administrators

The Royal College of Music reserves the right to audit networks and systems 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 likely to affect the College's reputation.

Other than any statutory obligation, the College will not be liable for any loss, damage or inconvenience arising directly or indirectly from the use of, or prevention of use of, any IT facility provided and/or managed by the College.

You are required to abide by the Joint Information Systems Committee (JISC) Acceptable Use Policy (AUP). A copy of the JISC AUP is available to read in the IT Office or on the intranet at the following https://community.jisc.ac.uk/library/acceptable-use-policy, should you require further detail.

2.4.4   Security and Proprietary Information

Users must not disclose their usernames or passwords to others and must keep them confidential. Users must not share user accounts.

All staff PCs, laptops and workstations should be secured by locking the Workstation (control-alt-delete then "lock workstation" for Windows users) when the system will be unattended. Students cannot lock Workstations and should ensure that they do not leave systems unattended when logged in.

Staff and students must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses or malware. Users must inform the RCM Technology Services immediately they suspect they may have received an infected email.

2.4.5 Unacceptable Use

The following activities are, in general, prohibited. Staff may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. IT Services staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances are staff or students of the Royal College of Music authorised to engage in any activity that is illegal under local or international law while utilising the Royal College of Music owned resources.

Under no circumstances should staff or students knowingly or willingly engage in the damaging of any College computer equipment. Damage (or theft) of College computer equipment is a very serious matter and will result in disciplinary proceedings against the perpetrator/s.

The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

2.4.6 Prohibited System and Network Activities
The following activities are strictly prohibited:

- Printing, display, storage or transmission of images, videos or text that could be considered offensive: e.g. material of a pornographic, sexist, racist, libellous, threatening, defamatory, terrorist nature or contrary to the RCM's equal opportunities policy.

- Unauthorized copying, including downloading from 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 Royal College of Music does not have an active licence is strictly prohibited.

- Playing of network games. This constitutes an inappropriate use of resources.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.
- Introduction of malicious programs into the network or server (e.g. viruses, spam or malware)
- Using Royal College of Music computing facilities to actively engage in procuring or transmitting material that constitutes sexual or other harassment.
- Making fraudulent offers of products, items, or services originating from any Royal College of Music account.
- Excessive or inappropriate use of RCM network bandwidth.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee or student is not an intended recipient or logging into a server or account that the employee or student is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing and forged routing information for malicious purposes.
- Any action that constitutes a Denial of Service attack. A Denial of Service attack is that which intentionally disrupts, prevents and/or removes access to computing services within the College or any external organisation.
- Port scanning or security scanning is expressly prohibited, except by the RCM Technology Services
- Executing any form of network monitoring, which will intercept data not intended for the employee's host, except by the RCM Technology Services.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, the Royal College of Music staff or students to parties outside the Royal College of Music.
- Users must not interrupt any virus checking activity. All RCM computing facilities have Anti-Virus software constantly monitoring the machine.
- You may not set up web sites on RCM computing facilities; publish pages on external web sites containing information relating to the RCM; enter into agreements on behalf of the RCM via a network or electronic communication system.
- Any action or lack of action which may interfere with security, other people's use, the Data Protection Act, serviceability of the network, or bring the College in to disrepute or breach of any Act or other activity which may be deemed to constitute misuse of the RCM computing facilities.

- The use of RCM IT facilities to engage in any behaviour which encourages extremism, radicalisation or terrorism, which may be, but not limited to, religious or political in nature; including through use of social media, or illegal access of terrorist materials online, is not permitted. This relates to the RCM's Prevent duties under the Counter Terrorism and Security (CT&S) Act 2015.

2.4.7 Prohibited Email and Communications Activities

Users should note that email messages form part of the public record and are therefore actionable.

The following activities are <u>strictly prohibited</u>:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
- Any form of harassment via email whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Misuse of distribution lists, such as: "spamming", modifying user lists without the list owners consent.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within the Royal College of Music's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the Royal College of Music or connected via the Royal College of Music's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

2.4.8 Blogs, social networking sites and other internet resources.

Social networking websites, such as Facebook, blogs, and other internet resources are good ways to keep in touch with friends and colleagues. However:

- The College and the Student Union take a very serious view of material that may offend or harass individuals or that might bring the College into disrepute.
- The College will take disciplinary action, including expulsion, against students in such circumstances.
- If you write something libellous, the individual concerned may take legal action against you.
- Make sure you take responsibility and think carefully about what you post to such sites.
- Be cautious as to what information you post on such sites, as it can be used to aid fraud.

2.5 Technology Accessibility Policy

2.5.1 Overview – The legislative context

The Equality Act 2010 replaced previous anti-discrimination law, consolidating it into a single act. The majority of the Act came into force on 1 October 2010 and extends to cover the rights of staff and students (including prospective staff and students) across nine 'protected characteristics': age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage and civil partnership, and pregnancy and maternity. The public sector equality duty entailed by the Act and which came into force on 5 April 2011, consists of a general duty, which is relevant to this policy.

The general duty has three aims; it requires the College to have due regard to the need to:

- eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Equality Act 2010
- advance equality of opportunity between people from different groups and
- foster good relations between people from different groups.

The UK Quality Code for Higher Education takes into account the fact that a student body will have a diversity of protected characteristics, which higher education providers consider when developing their approach to enabling student development and achievement. For this to be done effectively, the needs of individual students are to be considered. Provision is guided by principles of fairness, inclusion and accessibility, enabling access for people who have differing individual requirements, as well as eliminating arbitrary and unnecessary barriers. An inclusive environment anticipates the varied requirements of students and equity of access is achieved through inclusive design, wherever possible. In some circumstances, arrangements will need to be made to enable access for individuals. RCM aims to work in partnership with students to understand the implications of their specific needs.

2.5.2 Purpose

The overall strategic aim of the College's Technology Accessibility Policy is to provide a high-level of access to learning, teaching and administrative facilities to disabled students and staff, through appropriate IT services.

Examples of specific IT issues may include:
- Provision of assistive technology, such as: text enlargement software, large screens, Braille output and screen-reading software.
- Provision of accessible institutional services, including departmental, faculty and institutional Web sites

- Provision of accessible educational services, such as: Intranets, Virtual and Managed Learning Environments and other digital resources, including student handbooks and staff resources.

This policy, and the College's assistive IT provision, will be reviewed on an annual basis to ensure that the College's provision remains contemporary with developments in assistive technology.

2.5.3 Accessibility Policy

This policy applies to the facilities and services offered by the College's IT department.

The College's IT department will ensure that assistive technology is available across the College's IT estate and functions with the standard range of applications used by students and staff of the College.

In recognition of the specific requirements of technology in musical education a space will be maintained to provide software applications specific to music education for disabled users. This area will only accessible to staff and students with disabilities. In other areas where special provision has been made priority access will be available for disabled students.

The College shall ensure:

- That internal and external websites are accessible via assistive software;
- That Braille embossing facilities are available;
- That music editing software is available through assistive technology;
- That selected workstations are appropriately setup for disabled access.
- That IT Staff are appropriately trained to set up, maintain, and train users on use of assistive technology
- That the College actively monitors developments in assistive technology and informs directors and colleagues of developments that may be relevant to the College

2.5.4   Roles and Responsibilities

The Technology Manager, together with the Research Fellow in Musical and Visual Impairment and Student Services Manager, shall be responsible for promoting awareness of IT accessibility issues amongst staff and students of the College.

The Technology Manager shall be responsible for ensuring that accessible IT equipment is functioning correctly and does not pose a substantial disadvantage to disabled students.

All College Staff and Students will be responsible for reporting any unusable or damaged equipment to IT department staff as soon as possible. This is to ensure a minimal lack of service to students with disabilities.

All College Staff and Students are required to not disable or disrupt any element of assistive IT provision for disabled students

2.6 Network Access Policy

2.6.1 Purpose

The purpose of this policy is to outline the rules regarding the connection of computer equipment and other network devices to the Royal College of Music networking infrastructure. These rules are in place to protect the employees, students and the Royal College of Music. Inappropriate use exposes the College to risks including virus attacks, compromise of network systems and services, and legal issues.

2.6.2 Policy

College Computing Equipment

- No user is allowed to disconnect any College computing hardware from its assigned port on the College Network.
- No user is allowed to connect any College computing hardware to the College Network without the authorisation of RCM Technology.
- No user is allowed to install software without approval from the RCM Technology team. Wireless, Laptop and Handheld devices must meet the minimum standards for virus protection in 2.1.3 *Anti Virus*
- No user may move any IT equipment around the office. Office and equipment moves must be discussed with RCM Technology in advance to ensure that locations do not breach cable lengths or pose any risk to IT equipment. RCM Technology. Staff will disconnect and move equipment where required. In the case of Office moves, adequate notice in line with the RCM Technology SLA's via the IT Technology Service Desk is required.

Laptops and Other Network Devices

Because information contained on portable computers is especially vulnerable, special care should be exercised.

Any computer not owned by the Royal College of Music that requires connection to the RCM Computing Network, such as laptops, must follow the following rules.

- Owners/Operators of such equipment will be required to adhere to these policies and maintain current antivirus software, as in 2.3.1.
- Network devices must not be running spyware, as such activity can result in snooping, sniffing and interruption of network traffic. Devices discovered running in this way, will be removed from the network.
- RCM Laptop users are required to back-up critical data to the RCM Network on a regular basis.

Wireless LAN (WLAN) Connections

- Wireless network access is provided as a free service for students and staff on a best-endeavours basis. While we aim to for wide coverage, WiFi access may not be available in all areas.
- All Wireless LAN (WLAN) connections require user authentication before granting access to the RCM Network.
- All Wireless LAN (WLAN) devices must have current antivirus software, as in 2.3.1
- Configuration of Wireless LAN (WLAN) connections must be approved by RCM Technology Services.
- Further information on how to connect and work with various wireless devices can be found at: http://muse.rcm.ac.uk/sites/intranet/departments/ICT

Tablets, Smartphones, Mobile devices and personal laptops

- Staff and students are allowed to access the RCM Network using their own tablets, smartphones, mobiles devices and personal laptops. Documentation to assist with connecting to the RCM network with mobile devices is available on the IT Support Portal at: http://muse.rcm.ac.uk/sites/intranet/departments/ict
- The Royal College of Music Technology Service staff are only able to help with connecting devices to our services. For other issues, users must seek out the relevant help from their device provider, for example via the manufacturers support website.
- Smartphones, tablets and other mobile devices will have to authenticate with valid RCM credentials to receive network access.
- All staff and students using handheld devices to access RCM e-mail accounts must have a security PIN, password, biometric ID or device lock set on the device. This protects the device itself and the content in the event of theft or other misuse.
- All staff and students using handheld devices to access RCM e-mail accounts must, if the device is lost or stolen, report the loss to the RCM Technology IT department and attempt to erase the device using their link at: https://outlook.office365.com/owa/?path=/options/mobiledevice

2.6.3 Data security and portable devices

The security of personal, financial data as well as the General Data Protection Regulation (GDPR) and the colleges privacy policy is of paramount importance to the RCM Staff are personally responsible to make sure the data they use is secure.

- No personal or confidential financial data can be downloaded from the network drives where they are stored to any other place.
  No personal or confidential financial data can be removed from the RCM, in either paper or electronic format, without written permission from a director. For digital formats, this could include but is not limited to: – USB stick, phone, smartwatch, laptop, or tablet
- If data is to be accessed remotely via the VPN, it must not be downloaded to the local machine.
- If a personal mobile computing device or portable storage device is disposed of, make sure that the data are properly purged and destroyed. Seek advice from the RCM's Technology department

to ensure that the data is destroyed. Guidance is available in the university's Policy on Secure Disposal of IT Equipment and Information.

- If a device is lost or stolen, this must be reported to RCM Technology. To remotely wipe a device, log in to Office 365 and remote wipe in Mail / Settings. See the link above.
- If you suspect private or personal data has been or could be accessed by someone who is not authorised to do this, this must be reported immediately to the Technology Manager.

2.7 Remote Access Policy

2.7.1 Purpose
The purpose of this policy is to define standards for connecting to the Royal College of Music's network from any remote host.

2.7.2 Policy
Please review the following policies for details of acceptable use of the Royal College of Music's network and protecting information when accessing the corporate network via remote access methods:

a. Virtual Private Network (VPN) Policy

b. Laptop/Wireless/Network Access Policy

c. Acceptable Use Policy

For additional information regarding the Royal College of Music's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc go to the IT Support Portal: http://muse.rcm.ac.uk/sites/intranet/departments/ICT.

Remote Access will be controlled via password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.

Personal equipment that is used to connect to the Royal College of Music's networks must be an up to date operating system with patches, running a supported version of software and have anti-virus software.

Reconfiguration of a home user's equipment for the purpose of split tunnelling or dual homing is not permitted at any time.

Non-standard remote access hardware configurations must be approved by the RCM Technology Services.

2.7.3 Roles and Responsibilities

The Technology Manager is responsible for the strict control of remote access privileges.

Users with remote access privileges must ensure that their Royal College of Music owned or personal computer or workstation, which is remotely connected to the Royal College of Music's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

Staff must not use non-Royal College of Music email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct the Royal College of Music business, thereby ensuring that official business is never confused with personal business.

It is the responsibility of Royal College of Music employees, contractors, temporary staff and students with remote access privileges to the Royal College of Music's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the Royal College of Music.

Access to RCM online services by immediate household members through the Royal College of Music online services is forbidden. Users will be held responsible for any household member or any other person violating this policy.

Organisations or individuals who wish to implement non-standard Remote Access solutions to the Royal College of Music network must obtain prior approval from RCM Technology Services. This remote access will be recorded and managed by the IT team.

RCM Technology Services can only provide support for remote network access problems. Technical support for personal home computers are not the responsibility of RCM Technology Services.

2.8 VPN/Remote Gateway Policy

2.8.1 Purpose

The purpose of this policy is to provide guidelines for Virtual Private Network (VPN) connections to the Royal College of Music network.

2.8.2 Policy

Authorised Royal College of Music employees, contractors, temporary staff and students may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), co-ordinating installation, installing any required software, and paying associated fees.

- VPN use is controlled through the standard RCM login. However, VPN users may only connect to the terminal servers provided and not directly to the network.

- When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

- Dual (split) tunnelling is NOT permitted; only one network connection is allowed.

- VPN gateways will be set up and managed by Royal College of Music IT Services.

- VPN users will be automatically disconnected from Royal College of Music's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

- Only the RCM Technology Services approved VPN clients may be used.

2.8.3 Roles and Responsibilities

- It is the responsibility of employees, contractors, temporary staff and students with VPN privileges to ensure that unauthorized users are not allowed access to Royal College of Music internal networks.
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Royal College of Music's network, and as such are subject to the same rules and regulations that apply to Royal College of Music-owned equipment, i.e., their machines must be configured to comply with the RCM Technology Policies.

2.9 Auditing and Monitoring Policy

2.9.1 Purpose

To provide the authority for members of the RCM Technology to conduct or commission auditing and monitoring activities. The RCM Technology abides by the JISC Suggested Charter for System and Network Administrators, located at:

https://community.jisc.ac.uk/library/janet-services-documentation/suggested-charter-system-administrators

Monitoring and Auditing may be conducted to:

- Ensure compliance with software licensing requirements.
- Ensure integrity, confidentiality and availability of information and resources.
- Investigate possible security incidents ensure conformance to the Royal College of Music policies.
- Monitor user or system activity where appropriate.
- Provide real-time maintenance on a remote controlled basis.

2.9.2 Policy

When requested, and for the purpose of performing an audit, any access needed will be provided to members of the RCM Technology Services.

This access may include:

- User level and/or system level access to any computing or communications device by direct action or remote management.
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on the Royal College of Music equipment or premises.
- Access to work areas (offices, practice rooms, storage areas, etc.)
- Access to interactively monitor and log traffic on the Royal College of Music networks.

2.10 Data Management Policy

2.10.1 Purpose

RCM holds a variety of personal data regarding staff, students, donors and impersonal data such as research documents. This policy outlines the guidance and rules to support the management of electronic data residing on the College's IT systems. This document supplements the College's existing Data Protection Policy and Data Protection Guidance documents.

2.10.2 Policy
2.10.3 Electronic Data Storage

Electronic data must be stored on central RCM Technology servers or other appropriate location authorised by RCM Technology.

Primary copies of electronic databases must not be stored on desktop, laptop or other local devices. This is to ensure that data is secured in line with IT Security Policy and backed up as per RCM Technology procedures.

Removable media used by RCM Technology Services such as backup tapes must be securely stored at all times.

Sensitive data such as student records, payroll information, etc. must not be taken off site on removable media.

2.10.4 Databases

Major databases that are concurrently accessed by multiple people should be held in RCM's standard database application - Microsoft SQL Server. Technical staff responsible for database applications are authorised to decide what constitutes a major database. Minor databases, primarily those not needing concurrent access by multiple people may be in Microsoft Access or Microsoft Excel. Any proposed database must be approved by RCM Technology before any development.

2.10.5 Archiving

Data should be stored and archived in line with relevant legislation. Data should not be kept longer than is necessary.

2.10.6 Deletion of Data
- Data should be securely deleted once the need for it has passed in agreement with the data owner.
- IT equipment that stores data especially hard drives should be securely 'wiped' using before being disposed of, and if undertaken by a third party, a certificate of destruction obtained.

- A student's data e.g. e-mail, 'My Documents', etc. will be deleted on the 31st December after they leave the College.
- A staff member's data e.g. e-mail, 'My Documents', etc. will be deleted 60 days after they leave the College.
- Backup Tapes should be securely shredded once they approach end of life.

2.10.7 Roles and Responsibilities

The Technology Manager is responsible for:

- Ensuring that audits of stored data are carried out on a regular basis and that an inventory of data stores is maintained.
- That reasonable measures are taken, in line with data protection legislation, to ensure the integrity and security of systems storing electronic data.

The Technical Infrastructure Manager is responsible for:

- Data stores have sufficient capacity and resilience to prevent data loss.
- Backup procedures are robust enough to prevent data loss
- Backup procedures are adhered to

Data Owners, as defined in the RCM's Data Protection policy, must give their written authority before the Technology department delete data.

2.11 Backup Policy

2.11.1 Purpose

The College is reliant on the security and continuity of its electronic records and systems, A definition of the backup approach and the requirements of the College

2.11.2 Policy

The College uses four backup systems, for use in different scenarios. These are:

- Back Up Exec (traditional tape backup)
- Mirror to NAS
- Mirror To Azure (cloud)
- Volume Shadow Copy

Backup tasks are performed by the Support staff and are as follows:
- Checking the backup has been successful

- Maintaining the backup log
- Managing backup failure and escalating to the technical infrastructure manager or our managed support services provider (currently Nouveau) if needed
- Tape Management
- Housekeeping
- Validating backup data

The detailed procedures for these tasks are maintained in the Standard Operating Procedures manual, accessible by the whole team.

2.11.3 Roles

RCM Technology Manager is responsible for ensuring the College has an effective backup system
Technical Infrastructure Projects Officer is responsible for design and maintenance of the backup systems
RCM Deputy Technology Manager is responsible for monitoring day-to-day running
IT Service Desk Staff are responsible for the day to day running of the backup system

2.12 IT Environmental Policy

2.12.1 Overview

In the current climate of concern for the negative effects of energy consumption and improper waste management, the College's IT function has a clear responsibility to ensure a sustainable approach to environmental issues.

This responsibility is wide ranging and the College's IT function recognises, as a minimum level of performance, the need for compliance with environmental legislation. In addition, the College's IT function undertakes a commitment to continuous improvement in the areas of environmental management where it operates. This may involve the education and training of IT employees in environmental issues and in the environmental effects of their activities

2.12.2 Purpose

The purpose of this policy is to ensure that, in pursuit of its objective to support the provision of an inspirational learning experience, the Royal College of Music exploits technologies which are friendly to the environment wherever possible.

2.12.3 Policy

The College's IT function aims, wherever possible, to:

- Reduce the pollution, emissions and waste produced in the course of providing IT facilities to the College.

- Reduce the use of all raw materials, energy and supplies through the selection of suppliers with excellent 'green' credentials. This includes selecting technologies which contain energy saving features.
- Attach a high importance to all environmental matters, meeting and exceeding minimum regulatory requirements
- Consider environmental issues relating to technology in any estate development plans
- Operate a purchasing policy that gives priority to sustainability, energy efficiency and recycling
- Encourage the use of email and online activity as a replacement for unnecessary travel and/or excessive use of paper.
- Provide facilities for the minimisation of printing waste, through proper printer management and through facilities, such as: equipment capable of printing on both sides; equipment using reduced quantities of toner and recycling wherever possible printer consumables.
- Provide environmentally friendly solutions for redundant, obsolete and unwanted computers and IT equipment.
- Monitor closely the implementation of this policy, and report annually to the Information Strategy Group.

2.12.4 Roles and Responsibilities

The Technology Manager shall be responsible for ensuring compliance with all environmental legislative requirements.

All RCM Technology department staff shall be responsible for ensuring that the policy above is adhered to and for ensuring that system users comply with the requirements of this policy.

2.13 Backup Policy
2.13.1 Purpose
Robust backup and restore is an essential part of the College IT Services tasks, used both for day-to-day recovery of accidentally modified or deleted data, and for business continuity scenarios.

2.13.2 Policy

2.13.3 Roles and responsibilities
The Head of IT is accountable for the effectiveness of the backup systems.
The network manager is responsible for the design and day to day management of the systems.
IT Service desk staff are responsible for tape rotation and error monitoring and reporting.

2.14 Change Manage Management Policy

2.14.1 Purpose

A state of change is a characteristic of all information and telecommunications system. Change management is an essential procedure to develop the IT systems in a stable and secure manner. This policy ensures that this change is managed, authorised, recorded and has an audit trail.

2.14.2 Policy

Change management includes any software configuration changes, any updates, and any addition or removal of software or IT and telecoms systems that either
- Transforms, alters or modifies the operating environment
- Modifies the standard operating procedures

Infrastructure changes are planned and reviewed by the Network Manager with the Technology Manager. This planned change is recorded in the team project roadmap in Muse.

Changes made due to these plans, and any other change in the course of maintenance, is recorded in the Change Control database on Muse and is available to IT staff. The link is here:

http://muse.rcm.ac.uk/sites/intranet/Departments/IT/team%20site/Lists/Change%20Control/Summary.aspx

Changes are discussed in the fortnightly team meetings, and any changes that might cause service issues are flagged.

Software changes are planned and managed by the Business Applications Manager. These changes are authorised by the business owner of each system, who represents the staff users of these systems and manages and monitors access.

Business owners' change and authorisation records, and a separate record of Business Application versions are managed by the Business Applications and eLearning Manager and are accessible by the whole IT team via the team intranet.

2.14.3 Roles and Responsibilities
The Technology Manager is accountable for the change management procedure being followed.
The **Technical Infrastructure Projects Officer** is responsible for change management of network and infrastructure change management, and updating the Standard Operating Procedures as necessary.
The Business Applications Manager is responsible for business systems change management, and updating the Standard Operating Procedures as necessary.

2.15 Firewall policy
2.15.1 Purpose
The firewall policy ensures proper management of the College firewall, as the key gateway between the College IT systems and the public internet.

2.15.2 Policy

The firewall is managed and monitored by the **Technical Infrastructure Projects Officer** and our technical infrastructure provider Nouveau. Incidents are reported to the head of RCM Technology.

Outgoing connections

The default policy is to deny any non-registered outgoing internet traffic. Registering new outgoing services is requested via the IT helpdesk.

Incoming connections

The default policy for inbound traffic is to deny. Registering new incoming services is requested via the IT helpdesk.

Firewall access is allowed to the network manager and current maintenance Support Company.

Firewall change management is as follows:

- Before any changes are made, the current running configuration is copied to the RCM TFTP server
- All configuration changes are logged in the change log located on the RCM Intranet
- Any changes or additions to external IP addressed are registered in the External IP address list on the RCM Intranet
- After the changes have been made and saved to memory the running configuration is copied to the RCM TFTP

2.15

2.151 Purpose

The IT Asset Management policy ensures that all College IT hardware and software assets are tracked, locatable, and are accounted for through the whole lifecycle from order raising through to disposal.

The policy aims to fulfil the following seven goals:

- Uncover savings through process improvement and support for strategic decision making
- control the inventory
- Help IT staff ensure security of assets
- Enhance performance of assets and the life cycle management
- Enhance environmental benefits by ensuring that assets are procured, managed and disposed of in an environmentally efficient manner
- Ensure compliance with UK and EU waste disposal (WEEE) regulations
- Improve performance and availability of the IT systems

2.152 Policy

The policy covers management of hardware and software for computer and audio visual equipment in teaching rooms and in use around the College and in Prince Consort Village.

- IT procurement follows the standard College-wide procurement policy.

- IT assets are purchased from annually agreed capital and operational budgets, held by default by the IT Service and managed by the Head of the service. Centralised purchase ensures that assets are visible and that awareness of existing assets is present in the College. This reduces risks of items being duplicated, and allows for supplier management and bulk purchases.

- The section follows the College standard purchasing procedures, for credit card and purchase order purchases. Raising and processing of purchase orders and credit card purchases is undertaken by the IT Support Services Manager. However, the Technology Manager retains oversight of any purchases, authorises them by email, and monitors the budget.

- Assets are recorded in an excel document held in the IT Sharepoint site in the Inventory folder. This is maintained by the IT team with the following information as a minimum:

  - User category
  - Equipment type
  - Location
  - Serial number
  - Model
  - Purchase date
  - Warranty details

- Delivery notes for all purchases are retained by the section indefinitely.

- Hardware assets are disposed of through recycling companies following WEE regulations. Disposal is authorised by the Head of IT Services. The date and method of disposal is recorded in the asset database including:
  - Disposal date

  - Estimated value at disposal time

  - Method of disposal

  - Disposal company

  Certificates of destruction and transfer of ownership documents from the company used for waste disposal are recorded in the asset disposal file held in the IT office.

A London University Purchasing Consortium (LUPC) company will be used for disposal of un-needed assets where practical.

- Traceability tests of assets are undertaken by the Technology Manager every three months, tracing a minimum of twenty items from the purchase ledger to the current location of the asset. A report is submitted to the Director of Finance.

2.153 Roles

Technology Manager is responsible for managing the disposal of assets

Head of IT Services is responsible for authorising disposal of assets

Head of IT Service is accountable for asset management.

3. Appendix

3.1 Definitions
Application Administration Account: Any account that is for the administration of an application (e.g., SQL database administrator etc.)

JISC: Joint Information Services Committee. The UK's Education and Research computing network

CERT: Computer Emergency Response Team

Spam: Unauthorized and/or unsolicited electronic mass mailings to addresses outside the College

FTP: File Transfer Protocol

Email Header: Technical addressing information, normally unseen by users. Identifies sender and recipient information as well as structured routing information.

IPSec Concentrator: A device in which VPN connections are terminated.

Dual Homing: Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialling into AOL or other Internet service provider (ISP). Being on the Royal College of Music provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into the Royal College of Music and an ISP, depending on packet destination.

Remote Access: Any access to the Royal College of Music's corporate network through a non-the Royal College of Music controlled network, device, or medium.

Split-tunnelling: Simultaneous direct access to a non-the Royal College of Music network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into the Royal College of Music's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunnelling" through the Internet.

GDPR: General Data Protection Regulations are legal guidelines for receiving and processing personal information with in businesses.

BOYD: Bring Your Own Device.