Royal College of Music

ICT Services

ROYAL COLLEGE OF MUSIC London

ICT POLICIES

SOP Reference: RCM-GEN-POL-001	Effective date:	01/11/2007
Version Number: V1.9	Last Review date:	08/07/2016
Author: Mark Soole	Position:	Head of ICT Services
Approver: Kevin Porter	Position:	Deputy Director
	Next Review date	01/07/2017

Description:	This document contains important information on the policies in force for any users of the RCM network and RCM ICT services. All users are required to familiarise themselves with this document and the Acceptable Use Policy (AUP).
Technical Requirements:	Any computer capable of reading a PDF document. Link to Adobe Acrobat Reader download: http://www.adobe.com/products/acrobat/

Version History:	
V 1.0	Initial Issue by NW (10/10/2007)
V 1.1	Revised by NW (1/11/2007)
V 1.2	Updated by NW (19/11/2008)
V 1.3	Revised by NW (29/1/2010)
V1.7	Revised by MS (16/09/2014)
V1.9	Revised by MS (8/07/2016)

1. Introduction and Overview

1.1 Scope of ICT 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 ICT Services.

1.2 Purpose

The purpose of this document is to outline the policies applicable to the use of the Royal College of Music's ICT and network systems. All users of the Royal College of Music's ICT 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 Personnel & Training 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 ICT 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 ICT Security Policy

2.1.1 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

2.1.2 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 ICT 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 ICT security are adequately met.

The College wishes to promote effective and efficient ICT 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.

2.1.3 Policy

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

Physical Security

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

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

- RCM ICT Services 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.

IT Security Reviews and Penetration Testing

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

- '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.

- '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 ICT Services.

- RCM ICT Services will set user accounts for students to automatically disable on the 31st day of the 12th month after they leave the College.

- RCM ICT Services will set user accounts for staff to automatically disable 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 Head of ICT Services.

- 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 ICT Services personnel are permitted to purchase, install and delete software on computers owned by the College.

- Only RCM ICT Services 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 the network regularly to ensure software updates are applied.

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

2.1.4 Roles of Responsibilities

All College Staff and Students are responsible for promoting awareness of ICT 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 ICT Services as soon as possible.

The Head of ICT is responsible for approving IT Security policy and for ensuring that it is implemented.

RCM ICT Services 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 ICT Services are responsible for advising the ICT Steering Group on the appropriateness of and the College's compliance with this policy and its associated codes of practice.

The Head of ICT is responsible for the promotion of this policy throughout the College, analysis of the annual assessments of security and the reporting of these to the ICT Steering Group and maintaining records of misuse of the College systems.

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

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

The Network/Server Engineer is responsible for the pro-active management of the College's Network and Server devices.

The Head of ICT 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.

2.1.5

2.1.6 Reporting

RCM ICT Services 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 ICT Support Manager immediately who will advise the College on what action should be taken.

Users must inform the RCM ICT Services immediately of any suspected virus.

In the event of a suspected or actual breach of security, the ICT Support 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 Head of ICT (and in his/her absence other members of the Senior Management Team) have the authority to take whatever action is deemed necessary to protect the College against breaches of security.

2.2 Password Policy

2.2.1 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.

2.2.2 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.

2.2.3 Policy

- Users are responsible for the security of their passwords and accounts.
- All production system-level passwords must be part of the ICT Department administered global password management database.
- Remote Access to the Royal College of Music Networks will be controlled using a one-time password authentication.
- RCM ICT Services enforce the following User Account password rules:
    - All passwords must be changed on at least a quarterly basis
    - The password must contain no less than eight characters
    - The password must contain characters from two 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:
    - Do not use any of the examples as passwords in this document
    - 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)
    - The password is a word found in a dictionary (English or foreign)
    - Do not write usernames or passwords down or store them in a file on a computer
    - Passwords must not be the same as usernames
    - 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.)
    - Where possible, don't use the same password for various Royal College of Music access needs.
    - Do not share the Royal College of Music usernames or passwords with anyone.
    - Don't reveal a usernames or password in an email message
    - Do not use the "Remember Password" feature of applications (e.g. Outlook, Internet Explorer etc.)
    - If you suspect an account or password has been compromised, report the incident to ICT Department and change all passwords.

- Students and Staff are required to enroll with the RCM Password Portal Service

2.3 Acceptable Use Policy

2.3.1 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.

2.3.2 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.

2.3.3 General Use and Ownership

While the RCM ICT Services 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. The College cannot guarantee the privacy of information stored on any network device belonging to the Royal College of Music.

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 ICT Services. Private work use is not permitted if it is for personal gain. 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 ICT Services abide by the JANET-CERT Charter for System and Network Administrators, which can be found here:

http://www.ja.net/development/legal-and-regulatory/regulated-activities/charter-for-system-administrators.html

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 ICT facility provided and/or managed by the College.

You are required to abide by the Joint Academic Network (JANET) Acceptable Use Policy (AUP). A copy of the JANET AUP is available to read in the ICT Office or on the Intranet at the following address http://www.ja.net/company/policies/janet-aup.html, should you wish further detail.

2.3.4 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 XP users) when the system will be unattended. Students cannot lock Workstations and should ensure that they do not leave systems unattended when logged in.

E-mails and Newsgroup postings from a Royal College of Music email address should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Royal College of Music, unless posting is in the course of College duties.

Staff and Students must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. Users must inform the RCM ICT Services immediately they suspect they may have received an infected email.

2.3.5 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. ICT 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.

2.3.6 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, worms, trojan horses, e-mail bombs)

- 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 ICT Services

- Executing any form of network monitoring, which will intercept data not intended for the employee's host, except by the RCM ICT 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 ICT 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.

2.3.7 Email and Communications Activities

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

The following activities are strictly prohibited:

- 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).

2.3.8 Web logs (Blogs), social networking websites and other internet resources

Social networking websites, such as facebook.com, web logs (blogs), and other internet resources are good ways to keep in touch with friends and colleagues. However:

- The College and the Student Association 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.

2.4 IT Accessibility Policy

2.4.1 Overview - The legislative context

The Disability Discrimination Act (DDA) 1995 was amended to extend its scope to education with effect from September 2002. Under the Act it is unlawful to discriminate against a disabled student, potential student or applicant, and the responsibility for any case of discrimination lies with the governing body of the institution. In addition, the new Disability Equality Duty, which came into force in December 2006 means that any public body, including higher education institutions, will need to actively look at ways of ensuring that disabled people are treated equally.

Discrimination against disabled applicants or students can take place in either of two ways. For example, by:

- treating them "less favourably" than other people, or
- failing to make a "reasonable adjustment" when they are placed at a "substantial disadvantage", compared to other people, for a reason relating to their disability.

The Quality Assurance Agency (QAA) Code of Practice on Students with Disabilities sets out 24 'precepts' or standards that institutions are expected to meet. These precepts cover all areas of an institution's relationship with students, including all aspects of teaching and learning. It expects institutions to treat disabled students as an integral part of the academic community and provide for them as part of their core activities.

Examples of the requirements of this Code of Practice include:

- ICT provision for disabled people appearing as a regular agenda item on relevant committees, including those covering IT provision (precept 1)
- Ensuring disabled students have access to appropriate computer facilities; that laboratory and other equipment can be used by disabled people (precept 3)
- Accessible Web and Intranet sites, and alternative formats for programme details and other information (precept 4)
- Provision of equipment and other support for disabled students (including those not in receipt of any disabled students' allowances), based on an appropriate assessment of an individual's needs (precepts 6 and 18)
- Allowing disabled people to use ICT for examinations and assessment where appropriate (precept 13)

- Training staff to use relevant technology and to produce accessible electronic courseware. Ensuring IT staff have the time and skills to support assistive technology used by disabled people (precepts 15 and 17)

The DDA Act applies to the College's ICT facilities and requires an appropriate footprint of accessibility enabled ICT equipment to be provided to disabled students. This includes adjustments to ICT equipment to help alleviate any substantial disadvantage that might be experienced by disabled students without ICT accessibility provision.

Examples of specific ICT 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.

2.4.2 Purpose

The overall strategic aim of the College's ICT accessibility policy is to provide a high-level of access to learning facilities, through appropriate ICT services, to disabled students.

The College's ICT function strives to support the precepts detailed above and to ensure that the ICT provision available to disabled students meets the requirements of the Act, thereby ensuring an equal platform of opportunity for students, both with and without disabilities.

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

2.4.3 Policy

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

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

Recognising 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 be restricted and only accessible to staff and students with disabilities. In other areas where special provision has been made, such as lowered desks for wheelchair access, 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.

2.4.4 Roles and Responsibilities

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

The Head of ICT shall be responsible for ensuring that accessible ICT 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 ICT 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 ICT provision for disabled students.

2.5 Desktop\Laptop\Wireless & Handheld Devices Network Access Policy

2.5.1 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.

2.5.2 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 ICT Services.

- No user is allowed to connect any Non-College computing hardware to the College Network without the prior authorisation of the RCM ICT Services. Wireless, Laptop and Handheld devices must meet the minimum standards for virus protection in 2.1.3 *Anti Virus*

- No user may move any ICT equipment around the office. Office and equipment moves must be discussed with RCM ICT Services in advance to ensure that locations do not breach cable lengths or pose any risk to ICT equipment. RCM ICT Services Staff will disconnect and move equipment where required. In the case of Office moves, several days notice via the ICT Incident System 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 anti virus software, as in 2.3.1.

- Network devices must not be running in promiscuous mode, 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 an best-endeavours basis. Network access is restricted to 'hot-spot' areas and 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 anti virus software, as in 2.3.1

- Configuration of Wireless LAN (WLAN) connections must be approved by RCM ICT Services.

- Support information with 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 ICT Support Portal at: http://muse.rcm.ac.uk/sites/intranet/departments/ict

- The Royal College of Music ICT 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.

- PDAs, Smartphones and Mobiles 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 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 ICT department and attempt to erase

the device using their Royal College of Music web-based email portal at https://casarray.rcm.ac.uk/owa/

Data security and portable devices

The security of personal and financial data 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 ICT department to ensure that the data are 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 ICT. To remotely wipe a device, see the section Prompt reporting helps manage any risk of data going into the wrong hands.

- 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 Head of ICT.

2.6 Remote Access Policy

2.6.1 Purpose

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

2.6.2 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 RCM ICT Services website – www.rcm.ac.uk/ict or ICT 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.

Routers for dedicated ISDN lines configured for access to the Royal College of Music network must meet minimum authentication requirements of CHAP.

Personal equipment that is used to connect to the Royal College of Music's networks must meet the requirements of the Royal College of Music-owned equipment for remote access.

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

Frame Relay must meet minimum authentication requirements of DLCI standards.

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

2.6.3 Roles and Responsibilities

The ICT Support 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.

Users with remote access privileges to the Royal College of Music's corporate network 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.

General access to the Internet for recreational use by immediate household members through the Royal College of Music Network on personal computers is forbidden. Users will be held responsible for any family member violating any the Royal College of Music policies performing illegal activities.

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 ICT Services.

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

2.7 VPN Policy

2.7.1 Purpose

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

2.7.2 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 to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong pass phrase.
- 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 ICT 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.
- The VPN concentrator is limited to an absolute connection time of 24 hours.
- Only the RCM ICT Services approved VPN clients may be used.

2.7.3 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 ICT Services Policies.

2.8 Auditing and Monitoring Policy

2.8.1 Purpose

To provide the authority for members of the RCM ICT Services to conduct or commission auditing and monitoring activities. The RCM ICT Services abides by the JANET-CERT Charter for System and Network Administrators, located at:

http://www.ja.net/development/legal-and-regulatory/regulated-activities/charter-for-system-administrators.html

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.

2.8.2 Policy

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

2.9 Data Management Policy

2.9.1 Purpose

RCM holds a variety of data regarding staff, students, donor's 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 ICT systems. This document supplements the College's existing Data Protection Policy and Data Protection Guidance documents.

2.9.2 Policy

2.9.3 Electronic Data Storage

Electronic data must be stored on central RCM ICT servers located in the machine room or other appropriate location authorised by RCM ICT Services.

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 ICT Security Policy and backed up as per RCM ICT procedures.

Removable media used by RCM ICT 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.

2.9.4 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 ICT Services before any development.

2.9.5 Archiving

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

2.9.6 Deletion of Data

- Data should be securely deleted once the need for it has passed in agreement with the data owner.

- ICT equipment that stores data especially hard drives should be securely 'wiped' using the Gutmann Method before being disposed of.

- 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.

2.9.7 Roles and Responsibilities

The Head of ICT 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 Network/Server Engineer 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 ICT department delete data.

2.10 Backup Policy

2.10.1 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

2.10.2 Policy

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

- Doubletake (live data duplication to offsite servers)
- Acronis (complete back up of key servers)
- BackUp Exec (traditional tape backup)

Backup tasks are performed by the Support staff and are as follows:

- Checking the backup has been successful
- Maintaing the Backup log
- Managing backup failure and escalating to the network manager 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.

2.10.3 Roles

Head of ICT Services is responsible for ensuring the College has an effective backup system
Network Manager is responsible for design and maintenance of the backup systems
ICT Support Manager is responsible for monitoring day-to-day running
ICT Support Desk Staff are responsible for the day to day running of the backup system

2.11 IT Environmental Policy

2.11.1 Overview

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

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

2.11.2 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.

2.11.3 Policy

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

- Reduce the pollution, emissions and waste produced in the course of providing ICT 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.

2.11.4 Roles and Responsibilities

The Head of ICT shall be responsible for ensuring compliance with all environmental legislative requirements.

All RCM ICT 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.

2.12 Backup Policy

2.12.1 Purpose

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

2.12.2 Policy

2.12.3 Roles and responsibilities

The Head of ICT 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.

ICT Service desk staff are responsible for tape rotation and error monitoring and reporting.

2.13 Change Manage Management Policy

2.13.1 Purpose

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

2.13.2 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 Head of ICT. 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 ICT staff. The link is here:

http://muse.rcm.ac.uk/sites/intranet/Departments/ICT/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 and eLearning 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 ICT team via the team intranet.

2.13.3 Roles and Responsibilities

The Head of ICT is accountable for the change management procedure being followed.
The Network Manager is responsible for change management of network and infrastructure change management, and updating the Standard Operating Procedures as necessary.
The Business Application and eLearning manager is responsible for business systems change management, and updating the Standard Operating Procedures as necessary.

2.14 Firewall policy

2.14.1 Purpose

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

2.14.2 Policy

The firewall is managed and monitored by the network manager. Incidents are reported to the head of ICT Services.

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

Incoming connections
The default policy for inbound traffic is to deny. Registering new incoming services is requested via the ICT 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

3. Appendix

3.1 Definitions

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

JANET: Joint Academic NETwork. 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

Gutmann Method: A secure method of data destruction where data is overwritten 35 times. This method overwrites a hard drive taking into account the different encoding algorithms used by hard drive manufacturers.

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.

Cable Modem: Cable companies such as Virgin Media Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

CHAP: Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function.

DLCI: Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

Dial-in Modem: A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analogue signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

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 a 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.

DSL: Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Frame Relay: A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the
telephone company's network.

ISDN: There are two flavours of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signalling info.

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.