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		

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
-

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 re [illegible] take nT8 T.38 T1n T1n.24 841.921o2nT8 T.38 T1n T1n.24 8

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.

-

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 thed Stu(s)--

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, trustc2ioyal prf Mulege ocrude2 -0 0-3(ept)ndt(e o)[3(e o)-3C.08-3(')9(s)-5(es)-5(t)-1((e o)T)[a

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

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 abi7 fo

2.10 Data Management Policy

2.10.1 Purpose

- 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

- 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.

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

The firewall is managed and monitored by the **Technical Infrastructure Projects Officer** and our technical

A London University Purchasing Consortium (LUPC) company will be used for disposal of unneeded 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