RCS Information Security Policy

1. Introduction

1.1 The RCS recognises information as a key resource. Consequently, the information assets and the information systems associated with its production – servers, computers, databases, applications, networking infrastructure - must be protected in an appropriate and cost effective manner, in line with the JANET Security and Acceptable Use Policies

1.2 The Information Security Policy and the Conservatoire's procedures and structures will enable the Conservatoire to fulfil its responsibilities with regard to information security and enable a high quality service to be provided to staff, students and other clients. The Conservatoire believes that information security is an integral part of the business operation of the Conservatoire and that the adoption of information security will enable the Conservatoire to attain its strategic goals.

2. Definition & Objectives

2.1 For the purposes of this document, information security is defined in the provision of the following key concepts:-

Confidentiality: The Conservatoire must strive to protect information from unauthorised access and disclosure. Sensitive Information should only be accessed by those who have the authority to do so.

Availability: The systems must be robust and fault-tolerant to ensure that information is available to authorised users when it is required, within the limits of Conservatoire working practices and factors out with its control.

Integrity: The systems and the information that they contain must be up-to-date and be protected from being either deliberately or inadvertently modified.

2.2 The Conservatoire's objective with regard to information security is to use all reasonable, practical and appropriate security measures to maintain confidentiality, availability and integrity of information and their related information systems.

3. Applicability and Enforcement

3.1 The Information Security Policy applies to all members of the RCS – staff, students and appropriate third parties.

3.2 Compliance with the policy will be deemed to be part of the contract of employment for staff and third parties. Student enrolment and matriculation will ensure compliance via Conservatoire rules and regulations policy.

3.3 Failure to adhere and comply with the Conservatoires Information Security Policy will invoke disciplinary procedures.

3.4 This policy includes all home/remote working using RCS information and information systems.

3.5 RCS IT services may be accessed via RCS owned devices or via personally owned devices but this policy is applicable, regardless of the ownership of the device used.

3.6 Students and staff who have not been issued with an RCS laptop can still utilise all of the RCS's externally available services, which includes the full Office 365 suite of applications on their own devices. Users must always give due consideration to the risks of using personal devices to access RCS services and in particular, information classified as confidential, secure or containing personal information. Using your own device means that you will not be connected to the RCS wired network, but you are still bound by all the applicable RCS policies with regard to handling RCS data and information (see 3.5) If you are using your own device, the following regulations will apply:

You must:

- Not download or store any confidential or personal information or data sets onto any personal device or removable media device
- Run a current version of the devices operating system and have a recent security update installed
- Maintain your device with up-to-date anti-virus software, system patches and always keep all devices physically secure (devices provided by RCS must also be stored in a secure manner)
- Have appropriate password and encryption protection enabled and
- Adhere to the RCS Mobile Device Policy

4. Principles

4.1 The Conservatoire will adopt the following approach:

- Align with ISO27001, the international best practice information security management standard as a framework to produce the Information Security Policy. The Conservatoire will adopt the Information Controls within the standard which are pertinent and relevant to the institution and its practices.
- Take all reasonable and practical security measures to fulfil the adopted control mechanisms.
- Review the Information Security Policy on an annual basis. The Conservatoire will disseminate the Information Security Policy in an effective and appropriate manner.
- Whilst adhering to the Information Security Policy, the Conservatoire must ensure that in doing so, it complies with existing legislation. In particular, the UK GDPR and all applicable data protection legislation, the Copyright, Designs and Patents Act (1998), and the Freedom of Information (Scotland) Act 2002
- Align with the Scottish Government's Cyber Resilient Scotland: Strategic Framework

5. Overview of Information Security Controls

Information Security Responsibilities

5.1 All staff and students and appropriate third parties, have an obligation to protect our information assets and systems/services. Every person that handles information or

uses the Conservatoire's information systems is expected to adhere to the principles and practices within the Information Security Policy (and related policies) and to notify the nominated staff members of any security shortfalls or incidents.

5.2 The Conservatoire's Information Security Policy will be reviewed annually by the IT Governance Committee. The responsibility for disseminating the policy lies with the Head of Information Services and the Conservatoire's Human Resources department.

Policy Awareness & Information Security Training

5.3 The Information Security Policy will be made available to all staff, students and appropriate third parties. The Policy will be included in the induction process for new staff and student members and existing staff and students will be made aware of the policy's availability on the Conservatoire's portal and online training sites.

5.4 All members of the RCS community are mandated to undertake and complete the online Cyber Security and GDPR Training courses. Access to all RCS systems may be denied if this training isn't completed and successfully passed. This training is mandated by the Conservatoire Senior Management Team and the Board of Governors.

Authorised Use

5.5 Conservatoire IT facilities and information systems and services must only be used for authorised and legal purposes. The Conservatoire may monitor the use of IT systems and services and any person found to be using Conservatoire systems without authorisation or for unauthorised purposes, may be subject to disciplinary, and where appropriate, legal proceedings.

5.6 Authorised use is provided by the provision of a legitimate User ID and password. Centralised administration techniques are employed to ensure a suitable password length and uniqueness. Periodical password changes will be required and multi-factor authentication (MFA) will be used where appropriate.

5.7 User IDs and passwords are the sole responsibility of the intended authorised user and under no circumstances should user IDs and passwords be shared with other individuals.

5.8 Users should also consult the Conservatoire's Rules and Regulations, and in particular the Conservatoire's IT Acceptable Use Policy, and the Data Protection Policy.

Monitoring of Operational Logs

5.9 The Conservatoire shall only permit the inspection and monitoring of operational logs by authorised IT systems administrators. The Conservatoire may log all forms of IT use in order to identify and investigate technical or security related problems, and to provide an audit log in the event of unacceptable use, misconduct or criminal investigations. RCS also reserves the right to inspect any items of computer equipment connected to the network. Any IT equipment connected to the RCS network will be removed if it is deemed to be breaching RCS policy or otherwise interfering with the operation of the network. Any action to access or suspend any users account will only be taken where it has been authorised by a suitable RCS and/or HR representative.

Access to Conservatoire Records

5.10 In accordance with legislation as outlined in point 4.1 and elsewhere, the privacy of users files will be respected, however the Conservatoire reserves the right to utilise automated and manual processes to examine systems, directories, files and their contents, to ensure compliance with the law and with Conservatoire policies and regulations.

Hardware and Software purchasing

5.11 To ensure that the Conservatoire complies with copyright law, only licensed software products will be installed on Conservatoire information systems and services. The licensed products should only be installed by systems administrators and requests for additional licensed software should be made via the appropriate Line Manager to the Conservatoire IT Helpdesk. Members of the IT team will from time to time audit installed software applications and may remove unauthorised or unlicensed software from information systems. Unauthorised copying of software or the use of unauthorised products by staff, students or third parties may be grounds for disciplinary, and where appropriate, legal proceedings.

To maintain network integrity, and preserve asset management and procurement protocols, the IT Team are responsible for all IT hardware purchasing. No department or individual should purchase any IT equipment without prior consultation and approval from the IT Team. This includes any capital expenditure bids which include IT hardware or software.

6. Specific RCS Information Security Controls

Staff/Students/Third Party Responsibilities

6.1 All Staff/Students and authorised Third Parties must:

- Ensure that no unauthorised persons are allowed access to any of the Conservatoire's information
- Maintain network integrity by ensuring that only RCS equipment is connected to the RCS network
- Maintain data confidentiality and integrity by ensuring only RCS equipment and secure personal devices (see 3.6) are connected to RCS services
- Declare any potential conflicts of interest
- Not disclose passwords, user IDs or information security access procedures, except to authorised staff
- Not deliberately or recklessly introduce malware or viruses
- Not attempt to disrupt of circumvent any RCS IT security measures
- Embrace and co-operate in the implementation of the Information Security Policy and other dependent policies e.g. Mobile Device Security, Acceptable Use, Data Protection, Copyright etc.
- Not enable any auto-forwarding function from their RCS e-mail accounts to any private account. Conservatoire e-mail should be used for all Conservatoire related business and operations to ensure the security and integrity of RCS data
- Undertake all information and cyber security training packages as directed by the RCS IT Team and RCS Directors/HR department

Specialist Advice

6.2 Where it is deemed appropriate, the Head of Information Services and/or the IT Manager will seek specialist external advice with regard to security and legislation compliance issues. An external CISO is also employed by RCS to support information security.

Risk Management

6.3.1 As part of the Conservatoire's on-going Risk Management procedures, the Conservatoire's information systems will be subject to review and if needed, subsequent alteration in content or practice.

6.3.2 To assist in this process, all members of the IT Team must ensure that hardware and software asset registers are maintained and kept up-to-date, to ensure that the Conservatoire can assess the risk to its information systems with the most relevant criteria.

6.3.3 The IT Manager will ensure that the IT Disaster Recovery policy is updated to reflect any changes to the Conservatoire's information assets and systems.

Third Party Access

6.4 Third party access will only be granted to individuals/groups who agree as part of their conditions of contract to adhere to the Information Security Policy and the IT Acceptable Use Policy of the Conservatoire.

6.5 Where access to Conservatoire information systems is granted to third parties, members of the IT Team will invoke granular access controls i.e. the third party will be granted the minimum permissions to successfully complete the tasks and also undertake close supervision of the third party's actions.

6.6 If outsourcing is to be adopted, the Conservatoire must be satisfied that the third party can offer similar information security controls to those adopted by the Conservatoire. In addition, where it is deemed appropriate, data protection impact assessments (DPIA's), data sharing agreements (DSAs) and Service Level Agreements (SLAs) will be specified and adopted.

Equipment Security

6.7 The Conservatoire uses a centralised communications room to store its information systems and structured cabling i.e. switches and patch panels. This area is enhanced/secured by the following features:

- Air Conditioning
- Controlled access through key-code door

Equipment Maintenance

6.8 All Conservatoire information systems and related infrastructure will be covered by maintenance agreements with service response levels that are appropriate to the value

of the information stored within the information systems. This will be highlighted by the Conservatoire's continuing Risk Management processes.

Disposal of Equipment and Media

6.9 Equipment shall be disposed of under the authorisation of the IT Manager and will comply with current protocols. The removed/disposed equipment will then be removed from the asset register.

6.10 All devices will be formatted before disposal via certified disposal companies. Where this is not possible, the material will be physically destroyed.

6.11 Any sensitive or confidential information relating to information systems that is no longer required, or has been superseded, will be securely destroyed.

Security Incidents and Response Mechanisms

6.12 The IT Team will maintain a record of systems malfunctions and security incidents.

6.13 It is the duty of all staff/students/ authorised third parties to remain vigilant to cyber threats and inform the ITHelpdesk@rcs.ac.uk immediately of any suspected security incidents or potential security shortfalls.

6.14 In the case of data breaches (including suspected data breaches), individuals must report the incident to the RCS Data Protection Team immediately dataprotection@rcs.ac.uk. A breach investigation will be undertaken and the Conservatoire has a legal responsibility to inform the Information Commissioner's Office of any significant breaches within 72 hours.

6.15 The IT Team will be available during core hours to deal with major incidents.

6.16 The results of security incidents and responses will be documented by members of the IT Team and used within the continual security review process.

User Access Control

6.17. The HR Department, after collaborating with the appropriate line manager, will inform the IT Team with sufficient details for:

- new employees
- employees who are leaving the Conservatoire
- employees roles and permissions that should be modified

Correspondingly, the Registry Department will inform the IT Team with sufficient details for:

- New students
- Student leavers and graduates
- Changes in student status

6.18 Network access is granted to all approved staff as above and all staff are required to undertake an IT Induction. In order to maintain network integrity and comply with the account review process, the following conditions apply to network access:

- After 6 months of inactivity, user accounts will be blocked
- After 12 months of inactivity, user accounts will be deleted – all emails and data will be lost
- 3 attempts will be made to arrange a mandatory IT induction (the 3rd attempt will copy in the employee's line manager). If no response is received, the account will be deleted

6.19 Staff will only be given access to those services that they are required to utilise to fulfil their duties. Line managers must ensure that their staff have been adequately trained to ensure that the integrity of the information systems can be maintained.

6.20 If mobile devices are used for Conservatoire purposes, users must only load institutional data that is essential to their role in the Conservatoire and must abide by the requirements as laid out in this policy (including 3.6 above), the RCS Mobile Device Security Policy, Acceptable Use Policy and the Data Protection Policy.

Housekeeping

6.21 Unattended workstations and offices should be locked to prevent unauthorised access.

6.22 Information systems will have documented backup procedures. The IT Team will undertake regular check-ups of the validity of backups through test restores.

6.23 Information system owners must ensure that adequate end-user documentation exists for the operation of their systems.

Anti-Virus Configuration

6.24 The Conservatoire utilises centralised anti-virus and other cyber resilience detection protocols. The IT Team will ensure that these products are kept up-to-date and deployed to all Conservatoire PC's and servers.

6.25 All users must report any suspected viruses/cyber security incidents to the IT Team immediately.

6.26 Where it is deemed appropriate, the IT Team may delete files to minimise the risk of virus propagation.

6.27 When necessary, the IT team may invoke emergency procedures to isolate the Conservatoire network in order to maintain its integrity.

7. Protection of Personal Data & Individuals

7.1.1 The Conservatoire holds and processes information about employees, students, and other data subjects for academic, administrative and other purposes. When handling such information, the Conservatoire, and all staff or others who process or use any personal information, must comply with the Data Protection legislation which is set out in the Data Protection Policy and attending guidance documents. All members of the

RCS community have a responsibility to ensure an understanding and compliance with this legislation.

7.1.2 It is incumbent on all Conservatoire staff to ensure the integrity and confidentiality of Conservatoire information at all times. To this end, staff should refrain from storing or holding personal data about a data subjects on their personal equipment or mobile storage devices. The UK GDPR legislation defines personal data as information about a living individual (a “data subject”), who is identifiable by the information.

7.1.3 The IT Department will from time to time monitor Data Leakage of Sensitive Data as defined by the UK GDPR, the Conservatoire’s Data Protection Policy and the Conservatoire’s Risk Management Group.

7.1.4 Further to section 7.1.2, all users must ensure that any personal data which must to be taken / sent offsite for processing is adequately protected in terms of physical security and data encryption.

7.1.5 The Royal Conservatoire of Scotland has a statutory duty, under the Counter Terrorism and Security Act 2015, termed “PREVENT”. The purpose of this duty is to aid the process of preventing people being drawn into terrorism. In this regard, you must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. RCS reserves the right to block or monitor access to such material in line with the information security policy.