Royal Conservatoire of Scotland

IT Acceptable Use Policy

Document Revision History

Version No.	Version Date	Prepared By	Approved By	Summary
1.1	August 2012	Caroline Cochrane & Fraser Ross	Caroline Cochrane	RCS IT Acceptable Use Policy
1.2	August 2013		Caroline Cochrane	
1.3	May 2015		Caroline Cochrane	Updated Janet URL
1.4	Nov 2015		Caroline Cochrane	Inclusion of the Prevent Duty
1.5	July 2018		Caroline Cochrane	Update on data protection legislation
1.6	August 2019	C. Cochrane	ITGC	Reviewed & Updated
1.7	August 2020	C. Cochrane	ITGC	Reviewed & Updated

Royal Conservatoire of Scotland

Acceptable Use of RCS Information Technology

Introduction

The aim of this policy is to ensure that RCS IT facilities are used safely, lawfully and equitably. The RCS seeks to promote and facilitate the proper and extensive use of Information Technology in the interests of learning, teaching, research and business operations. Whilst the tradition of academic freedom will be fully respected, this also requires responsible and legal use of the technologies and facilities made available to students, staff and partners of the RCS. Acceptable use of IT is a team effort involving the participation and support of every RCS member of staff and student who deals with information and/or information systems. It is the responsibility of every technology user to know these guidelines, and conduct their activities accordingly.

Scope

The policy covers the use of all technology facilities provided by the RCS. The facilities include use of the internet and all RCS IT systems and infrastructure together with all software, operating systems, databases, network accounts, e-mail and any other related collaboration and networking components. This policy should be read in conjunction with RCS's Information Security Policy. This policy applies to all students, employees, contractors, consultants, temporaries and other members of staff at RCS. It should be read and understood by all users accessing RCS information, IT systems, networks or software using any RCS or personally owned device, either on RCS premises, or elsewhere. This policy should be interpreted so as to encompass new and developing technologies and uses, which may not be explicitly referred to in the policy.

Acceptable Use of IT

Acceptable use is defined as any use that supports the Conservatoire's teaching, learning, research, business and administrative activities, and does not meet the definition of Prohibited Use (Section 3). An implication of this policy is that compliance with it will ensure that computer use contributes to staff effectiveness and to the student learning experience.

1. Staff

1.1.1 RCS computers are connected to the JANET network to enable access to the Internet and to web email services. Users of such computers are also bound by the JANET Acceptable Use and the JANET Security Policy https://community.ja.net/library/janet-policies

1.2 RCS email accounts (address ending'@RCS.ac.uk') should be used for RCS business only. Messages using these addresses will carry a disclaimer and signature information identifying the sender, their job title and contact information.

1.3 For the purpose of 1.2, RCS business is deemed to include any messages relating to professional RCS matters or RCS-related staff activity. RCS IT systems or credentials must not be used by staff for any private enterprise or commercial gain

1.4 Staff should treat email as written communication and ensure that comments contained in an email comply with Section 3 below. Staff should ensure their email is not susceptible to forming grounds for any complaint or legal action against the individual or the Conservatoire. Staff should be fully aware of their obligation under the UK Data Protection Act 2018 & the EU General Data Protection Regulations (GDPR) regarding data privacy and be aware that all recorded information may be subject to Freedom of Information requests and/or Data Subject Access requests.

1.5 Staff wishing to use RCS machines for personal web or email access may do so outside their normal working hours provided that a machine is available and that its use complies with the Acceptable Use Policy. Staff should be aware that use of email and the web on RCS machines can be monitored in accordance with the Conservatoire's Information Security Policy.

1.6 RCS computers are pre-loaded with standard desktop software. The IT staff will acquire and load any other software requested by a member of staff for their work, provided that it is compatible with existing packages and approved by budget holders.

1.7 Staff may not download and install computer programs from the Internet or open unsecure files contained in email messages without first consulting the IT staff.

1.8 Staff should be aware that any customisation of the Windows desktop display carried out by them may be lost when systems upgrades are carried out.

1.9 The IT staff will make every effort to inform staff in advance when access to a computer is required and to fit in with individual preferences for times of access. It may however, be necessary to access a computer without the knowledge of a member of staff if they cannot be contacted. In these circumstances, the IT staff will subsequently inform the staff member that the computer has been accessed and why.

2. Students

2.1 RCS computers are connected to the JANET network to enable access to the Internet and to web email services. Users of such computers are also bound by the JANET Acceptable Use and the JANET Security Policy https://community.jisc.ac.uk/library/janet-policies

2.2 Students should treat email as written communication and ensure that comments contained in an email comply with Section 3 below. Students should ensure their email is not susceptible to forming grounds for any complaint or legal action against the individual or the Conservatoire.

2.3 Students may not download and install computer programs from the Internet or open unsecure files contained in email messages without first consulting the IT staff.

2.5 Students should always endeavor to store academic work on the appropriate drive (Office365 OneDrive) as local storage may result in loss of data. All data stored should be work related and can be monitored.

2.6 The IT staff will not provide support for problems arising out of use of computers for non-course related activities, or for software not authorised through the Conservatoire's standard procedures.

2.7 Computers are provided to enable students to carry out their studies effectively. The number of machines available is limited and therefore students should be mindful of using facilities for non-course related activities during peak periods. Personal internet or email access is acceptable provided that a machine is available and that its use complies with the Acceptable Use Policy. Students should be aware that use of email and the web on RCS machines can be monitored in accordance with the Conservatoire's Information Security Policy.

3. Prohibited Use – *STAFF & STUDENTS*

To safeguard the Conservatoire and individual users, the following are unacceptable and are likely to lead to disciplinary action being taken.

- Any act which contravenes any laws, RCS policies or regulations
- Gaining or attempting to gain unauthorised access to accounts and passwords
- Gaining or attempting to gain access to restricted areas without appropriate authorisation
- Disrupting the work of other users
- Wasting network resources, or wasting time of staff involved in the support of such resources
- Violating the privacy of other users
- Using the network connection in a way that denies other users access to computer systems
- Send spam (unsolicited bulk e-mail) or use RCS mailings lists other than for legitimate RCS purposes related to RCS activities
- Using personal email accounts instead of an RCS staff email account to conduct RCS business, or automatically forwarding emails from a staff email account to a personal account
- Creating, transmitting, downloading, browsing, viewing, sharing, reproducing or accessing, any image, material or other data of any kind which contains unacceptable content, including but not limited to: sexually explicit messages, images, cartoons, jokes or any other material of a sexual nature; any other content which may offend, harass, provoke, demean, degrade or threaten any other person whether on grounds of sex, sexual orientation, age, race, national origin, disability, religious, political belief, or otherwise:

    - Promotes or causes violence

- Is illegal
- Is defamatory, slanderous, libellous or derogatory
- Includes pornography, hate speech, violence or promotion of terrorism;
- intentionally or recklessly introduces any form of spyware, computer virus or other potentially malicious software to the Conservatoire or any other party or is designed to corrupt or destroy the data of other users
- Involves private business purposes or conflicts with the Conservatoire's interests or policies
- Infringes or may infringe the intellectual property or other rights of others, such as copying or transmitting (without authority) materials accessed on the Internet
- Involves the disclosure of information that is confidential to the Conservatoire or its users
- Benefits any political or commercial organisation

These restrictions apply to both work and personal use. Limited personal use of electronic mail and the internet is inevitable, but this must not be excessive, nor interfere with business needs or normal operations and must comply with Section 3 above.

It is recognised that certain staff, in connection with their work, may require to access to what could be classed as inappropriate material. Such exceptions must be registered in advance and approved through the appropriate Conservatoire Director and the IT department.

4. Applicable Laws, Licenses and Regulations

4.1 All users must comply with the UK Data Protection Act (2018), the EU GDPR and the Freedom of Information (Scotland) Act 2002, insofar as it is relevant to their computing activities. The RCS Data Protection Policy is included in the Conservatoire Rules and Regulations and further information can be found on the RCS Portal.

4.2 All users must comply with the provisions of the Copyright, Designs and Patents Act 1998, the Computer Misuse Act 1990 and other relevant statutes.

4.3 No user may copy programs or data which are copyright or subject to restrictive license agreements on removable media such USB or on to portable hardrives. Users should assume that ALL software is subject to a restriction unless there is a clear indication that this is not the case.

4.4 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 addition to the misuse outlined above, 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.

5. System Security and Access Restrictions

5.1 A user must log on to the network system or stand-alone machines only under a username or into an area to which they have authorized access. Logging-in to a machine using someone else's username is a disciplinary offence.

5.2 It is the responsibility of all users to maintain the security of their own passwords. Any user who fails to take reasonable steps to do so commits a disciplinary offence and may be held liable for any consequences which follow if another person makes use of them. Failure to maintain security of a password may lead to a suspension of use.

5.3 Anyone authorised to use the computing resources shall treat as privileged any information about individuals or organisations which may become available through access to those resources. The disclosure of such information to third parties is a disciplinary offence.

5.4 The IT staff will make every effort to inform users well in advance when network downtime is required. It may, however, be necessary to withdraw access to the network without warning if a security issue arises or in the case of equipment failure.

6. Disciplinary Action

Any breach of this policy by authorised users will normally be dealt with under the appropriate Disciplinary Procedures. Users may have their authorisation to use Conservatoire computing facilities or remote facilities immediately suspended pending an investigation by an authorised person in the Conservatoire. The Conservatoire may, if it considers it necessary, use an external agency to carry out appropriate investigations in cases of misuse. In the event of loss being incurred by the Conservatoire or members of the Conservatoire as a result of breach of these rules by a user, that user may be held responsible for the reimbursement of that loss. In the case of students, RCS will accept no responsibility for the effect disciplinary action might have on a student’s academic progress and achievement.