1. Organisational

1.7. Internet, Email and Computer Use Policy

This policy must be read in conjunction with Riverina Conservatorium of Music (RCM) Organisational Policies General Outline, Definitions and Relevant Legislations.

1. Purpose

a. The RCM recognises the usefulness of internet, email and computer facilities as research, communications and work tools. This policy sets out the appropriate standards of behaviour for users accessing all online and computer facilities or when making reference to the RCM on external sites.

b. The RCM provides internet access via ethernet and Wi-Fi network at the RCM for RCM staff only via the RCM Staff login. Staff may connect to this network with private computers at their own risk. All computers connected to the network must meet the requirements of this policy.

c. The RCM provides internet access via ethernet and Wi-Fi network at the RCM for students and the RCM community via the RCM Guest login. Students and the RCM Community may connect to this network with private computers at their own risk. All computers connected to the network must meet the requirements of this policy.

d. At all times when accessing or using RCM internet, email or computer facilities, users must ensure that they comply with this policy. It is the user's responsibility to ensure that they use RCM internet, email and computer facilities in a lawful and professional manner.

e. This policy does not form part of an employee's contract of employment or other user's contract.

2. Additional Definitions

a. **User:** all RCM employee and contractors who access or use the RCM Internet, email and computer facilities by any means.

b. **Confidential Information:**

i. Any confidential information relating to, or belonging to the RCM, including any such information relating to:

1. Customers or clients
2. Customer lists or requirements
3. Suppliers
4. Terms of trade
5. Pricing lists or pricing structures
6. Marketing information and plans
7. Intellectual Property
8. Inventions
9. Business plan or dealings
10. Plans, designs, product lines

11. Any document identified as being confidential by the RCM
12. Research activities and
13. Software and the source code of any such software

ii. Confidential Information does not include information that:
    1. is generally available in the public domain or
    2. was known by you prior to the disclosure by the RCM, its employees, representatives or associates.

c. Computer Network: Includes all RCM's internet, email and computer facilities which are used by users, inside and outside working hours, in the workplace of the RCM or at any other place while performing work for the RCM. It includes, but is not limited to, desktop computers, laptop computers, iPads, tablets, other handheld electronic devices, smart phones and similar products, and any other means of accessing the RCM's email, internet and computer facilities.

d. Intellectual Property: all forms of intellectual property rights throughout the world including copyright, patent, design, trade mark, trade name, and all confidential information and including know-how and trade secrets.

e. Multiple Factor Authentication (MFA): is a multi-step account login process that requires users to enter more information than just a password. For example, along with the password, users might be asked to enter a code sent to their email or mobile phone.

f. Browser: is an application for accessing websites.

g. IT: Information Technology. Is the science and activity of using computers and software to store and send information.

3. Application of Policy

a. This policy applies to all RCM employees and contractors who access or use the RCM internet, email and computer facilities by any means.

b. It applies to the use of all RCM internet, email and computer facilities inside and outside working hours and inside and outside the workplace. This includes portable computers (including all Personal Digital Assistants (PDAs), mobile phones and similar devices), and any other means of accessing the RCM email and internet facilities, for example, a personal home computer or mobile phone which has access to or is used to communicate with the RCM's IT systems.

c. It applies to users who contribute to external sites that identify themselves as associated with the RCM**.**

4. Details

a. Users are entitled to use the RCM internet, email and computer facilities for legitimate business use only.

b. Users are permitted to use internet, email and computer facilities for limited and reasonable personal use, however any such personal use must not impact upon the user's work performance or RCM resources or violate this policy or any other RCM policy or legislation. Further, the users must not use internet, email and

computer facilities for personal use if that use interferes with the efficient business operation of the RCM.

c. The RCM gives no warranty or assurance about the confidentiality or privacy of any personal information disclosed by a user in the course of using the computer network for the users personal purposes.

4.1 Guidelines for the use of Internet, Email and Computer facilities

a. Users must comply with the following guidelines when using internet, email and computer facilities;-

i. Users must use their own user name/ login code and their own unique password when accessing the RCM internet, email and computer facilities.

ii. Users must not save passwords in their browsers.

iii. Users must use multiple factor authentication when accessing RCM data.

iv. Users in possession of RCM computing equipment (including, but not restricted to, mobile phones, PDAs and laptop computers) must at all times ensure that it is stored or placed in areas with minimal possibility of theft or damage.

v. Users should protect their user name/ login codes and password information at all times and not divulge such information to any other person, unless it is necessary to do so for legitimate business reasons.

vi. Users should ensure that they log off from internet and email, and lock the computer or shut down the computer when leaving the computer equipment unattended to ensure that others do not have access to their internet, email and computer facilities.

vii. If a user receives an email that they suspect contains a virus, they should not open the email or attachment to the email and should immediately report the incident to the Executive Team member(s).

viii. If a user receives an email; the content of which (including images, videos, software, materials or text) is in breach of this policy, the user must report the matter immediately to the RCM Executive Team member(s). The user must not forward the email to any other person. The user must not delete or move the email until the Executive Team member(s) instructs the user to do so.

ix. Users will utilise available email functions as follows and in accordance with the RCM Privacy & Confidentiality Policy and the RCM Code of Conduct:-

1. Carbon Copy (cc): to include all persons directly related to, or whom should be advised of, details within an email being sent.
2. Blind Carbon Copy (bcc): for sending of any public announcements.
3. Reply: the reply function is to be used to respond to emails to ensure the full correspondence/conversation is included and can be referred to.
4. Reply-all: Where the email is of a conversational nature (and not a general announcement), then all recipients should be maintained in the conversation.
5. Forwarding of emails: is to be utilised where it is deemed that a person needs to be made aware of an email for business or operational purposes.

x. Users utilising non-RCM computing equipment to connect to the RCM's Network must:

1. Maintain an up-to-date Anti-Virus program.
2. Ensure their firewall is turned on.
3. Must turn any automatic update systems to OFF. This includes System updates. Anti-Virus updates are exempted from this clause.

4.2 Prohibited Content

a. Certain behaviour is considered to be inappropriate use of the RCM internet, email and computer facilities and is strictly prohibited. Examples of such prohibited content include the following:

b. Users must not send (or cause to be sent), upload, download, use, retrieve or access any email, software, images, videos or other Internet material that:-

i. Is obscene, offensive, or inappropriate. This includes text, images, sound, videos or any other material, sent either in an email or in an attachment to an email, or through a link to an internet site (URL). For example, any material of a sexual nature, indecent or pornographic material;

ii. Causes insult, offence, intimidation, or humiliation by reason of unlawful harassment or discrimination;

iii. Is defamatory or incurs liability or adversely impacts on the image or reputation of the RCM. A defamatory message or material is defined to insult or lower the reputation of a person or group of people;

iv. Is otherwise illegal, unlawful or inappropriate;

v. Affects the performance of, or causes damage to the RCM computer system in any way;

vi. Gives the impression of or is representing, giving opinions or making statements on behalf of the RCM without the express authority of the RCM. Further, users must not transmit or send documents or emails (in any format) to any external parties or organisation unless it is required as part of the performance of his/her duties.

c. Users must not use the RCM's internet, email and/or computers facilities to:-

i. Violate copyright or other intellectual property rights. Computer software that is protected by copyright is not to be copied from, or into, or by using RCM computing facilities except as permitted by law or by contract with the owner of the copyright.

ii. Contradict the RCM Privacy & Confidentiality Policy and the RCM Code of Conduct.

iii. Create any legal or contractual obligations on behalf of the RCM unless expressly authorised by the RCM Board of Management.

iv. Disclose any confidential information of the RCM or its clients or suppliers of the RCM unless expressly authorised to do so by the RCM Board of Management.

v. Install software or run unknown or unapproved programs in RCM computers. Under no circumstances should users modify the software or hardware environments on RCM Computer systems.

vi. Gain unauthorised access (hacking) into any other computer within the RCM or outside the RCM or attempt to deprive other Users of access to or use of any RCM computing systems.

vii. Send or cause to be sent chain or SPAM Emails in any format;

vii. Use RCM internet, email and computer facilities during working hours for personal gain or personal commercial enterprises. For example, running a personal business using RCM computers, internet or email facilities.

d. Child Protection and RCM IT

i. Any staff interacting with children or young people outside the scope of this clause does so at their own risk.

ii. RCM Staff must not:

iii. Use RCM internet, email and computer facilities to communicate socially with children or young people regardless of whether they are a student at the RCM or not.

iv. Exemptions as follows:

1. Legitimate business communication. Staff are advised to store copies of all communication with students.

2. Communication with student family members.

e. RCM Staff must not engage in online communication or relationships with children or young people who are or have been students of the RCM through any online social networking tool or chat room. This includes, but is not restricted to, facebook, twitter, instagram, snapchat, tiktok or Skype (Skype and other telecommunications tools may be used for legitimate RCM activities including the provision of video-conferenced lessons and lesson organisation).

f. Users must not use another user's RCM computer, internet or email facilities (including passwords and login details) for any reason without the expressed permission of the user.

4.3 Standards in relation to sites not operated by the RCM

a. The RCM acknowledges that users have the right to contribute content to public communications on websites not operated by the RCM, such as social networking sites like LinkedIn, Facebook or YouTube. However, as posting content on social media has the potential to cause damage to the RCM, employees, students/parents/guardians, suppliers and patrons, the following provisions apply to all users:

i. As it may be possible for any user of an external site to conduct a search that will identify any comments about the RCM, users must not publish any material which identifies themselves or others as being associated with the RCM, except in the case of RCM approved postings.

ii. Users must not publish any material that could potentially subject the RCM to legal liability. Examples include, but are not limited to, copyright infringement, child protection issues, defamation, or discrimination proceedings.

iii. If it comes to the RCM's attention that a user has made inappropriate and/or unauthorised comments about the RCM or an RCM employee, the RCM may choose to take disciplinary action against a user as outlined in this Policy.

4.4 Breach of this Policy

a. Any breach of this policy may result in disciplinary action that may include immediate termination of employment (or for contractors, the termination or non-renewal of contractual arrangements).

b. Other disciplinary action that may be taken includes, but is not limited to, issuing a warning, suspension or disconnection of access to internet, email and computer use (whether permanently or on a temporary basis) as determined by the RCM Executive Team.

5. Variations

a. If a worker is unsure about any matter covered by this Policy, they should seek the assistance of the Executive Team Member(s).

b. *The RCM reserves the right to vary, replace or terminate this policy from time to time.*

Policy version and revision information

Policy drafted by: Hamish Tait with advice from RCM legal representatives.
Policy drafted: November/December 2007
Policy Ratified by Board: December 2007
Policy Reviewed by Hamish Tait January 2010.
Reviewed policy ratified by Board: March 2010
Policy Reviewed by Staff Representatives to the Board May 2010
Reviewed policy ratified by the Board of Management May 2010
Policy Reviewed by: Venita Riordan, Emily Blake & Amanda Gibson
Policy reviewed: September 2023
Reviewed policy ratified by RCM Board of Directors: 20th March 2024