ROYAL ACADEMY OF DANCE

Information Technology (IT) Acceptable Use Policy

RAD - Information Technology (IT) Acceptable Use Policy

Introduction

This policy applies to all use of IT services administered by the RAD. The RAD's IT services are coordinated and managed by the Information Technology (IT) Department. It is the responsibility of each individual user to ensure that they use RAD IT services in an acceptable manner in accordance with all RAD policies and current legislation. RAD IT services may be withdrawn from individuals and disciplinary action may be taken if the terms of this policy are not observed. In severe cases, the Police and other authorities may be notified.

Acceptable Use

RAD IT services may be used for any legal activity to support teaching, learning, research, administration and approved business activities of the RAD. Occasional and limited personal use is permitted but such use is a privilege and not a right. See Appendices A and B for guidance on acceptable and unacceptable personal use. If, for legitimate teaching or research purposes, access is required to material normally deemed as unacceptable (see Appendix B for examples) then a request for such access must be made by the relevant department to the Head of IT.

Unacceptable Use

Unacceptable use includes:

i any illegal or unlawful activity;

ii unauthorised use of IT services;

iii any activity or behaviour which compromises security;

iv any activity or behaviour which adversely affects IT services;

v any activity or behaviour which adversely impacts on the RAD.

Examples of unacceptable use of RAD IT services are given in Appendix B.

Responsibilities

If any user of RAD IT services discovers a breach of this policy or any other RAD IT Policy they must report it to the IT Department in the first instance.

IT security incidents or discovery of IT security weaknesses or software malfunction should be reported to the IT Department in the first instance. Where deemed necessary (for example, in the event of a data breach) the IT Department will inform the Data Controller and the Procedure for Data Security Breaches will be followed.

Users are responsible for the security of any RAD accounts allocated to them. Accounts must not be used by anyone except the allocated account holder. Users must keep their passwords confidential and not disclose them to others, including to RAD IT staff, or attempt to obtain or use anyone else's account logon details. If users believe that a password to one of their allocated accounts is known to others then they must change that password immediately.

Unless directly allocated to them by the RAD's Wireless Network Guest System, users must treat any password provided to them as temporary and change it on first use.

Users should follow good security practices in the selection and use of passwords/passphrases. Passphrases are composed of a sequence of words or text so are, generally, preferable to passwords as they are longer in length.

For more information please see the RAD Password Policy

Users should ensure that unattended equipment has appropriate security protection:

i For mobile computing equipment, please ensure that it is appropriately secured against theft and unauthorised use (e.g. password protected).

ii For RAD computing equipment provided for employee use, if you are leaving it unattended then you must either log off your session or lock the session until you return.

iii For RAD computing equipment provided for student use, you must log off if you are leaving it unattended.

iv Log off when your session is finished. Do not just switch off the equipment.

Users must not use any technologies which directly or indirectly interfere with the RAD's services or are designed to bypass RAD IT Policies

Users who use personally-owned devices to access RAD IT services must ensure that their usage is compliant with all RAD policies. It is recommended that all such devices use, where possible, a device password (or equivalent) and data storage encryption to prevent unauthorised access.

The use of personally-owned devices by employees for RAD business purposes should be avoided. Employees must not use personally-owned devices to hold any RAD data that is sensitive, personal, confidential or of commercial value.

Some RAD IT services mandate the use of Meraki Mobile Device Management (MDM) software before the service can be accessed. By agreeing to install this MDM software on personally-owned devices you authorise the RAD to remotely manage your device in order to secure its usage of RAD IT services. If deemed necessary by IT this may include the remote wiping of RAD data and applications from your device. The RAD accepts no liability if personally-owned data and/or applications are lost as part of this process.

Users must also comply with the RAD Procedure for Security of Personal Data when using RAD IT services or personally owned devices.

Allowing and Disallowing Access to IT Services

Student accounts are created automatically after enrolment of the student and remain active until the end of the course or receipt by IT of notification of withdrawal. Student passwords are issued in accordance with the current procedures.

Employee or student accounts may be locked by authorisation of the Head of IT (or appropriate Senior Management).

Accounts will not be deleted purely on the instructions of the individual who is leaving. It is the responsibility of the appropriate line-manager to identify and protect any important business information stored and managed by the person leaving. Centrally controlled accounts will on the departure of an employee be disabled, and any associated files or emails kept for a period of 56 days. The HR Department informs the IT Department immediately upon receiving notification of an employee's resignation and the employee's line manager is responsible for dentifying and securing all information at risk of being lost. If necessary, IT will work with Departments and to provide access.

Once a user has left employment or study with the RAD then they have no legal right to continue to use any accounts on the RAD's computer systems that had been allocated to them, such as email. Additionally, licensing restrictions may also forbid such access.

Auditing and Administrative Access

Under UK law, employers are generally liable for what their employees do in the course of their work. The RAD also needs to ensure that users are not infringing RAD Policy.

IT reserves the right of access to data stored in or transmitted by RAD IT Services and audit logs on RAD equipment and RAD systems (including cloud-based services) for legitimate purposes, such as investigation of complaints or misuse. Contents and audit logs for both sent and received content may be inspected (including any personal content) at any time without notice. Such access requires authorisation by the Head of IT (or appropriate deputy).

IT will endeavour to maintain privacy of users' data. However, there may be special cases where it is essential that data is accessed due to, for example, illness of the owner. In these instances, on the request of the relevant Department Head, Director or Head of HR and on the authorisation of the Head of IT (or appropriate deputy), IT may locate and make available the data for access by a nominated employee. The owner of the data will be notified..

It may be necessary for certain authorised members of IT to obtain access to the contents of users' data in the course of system administration. Any knowledge thus obtained will not be communicated to others, unless required for system administration purposes or an infringement to RAD Policy is discovered.

IT reserves the right to take special actions in administering users' data if this is essential to preserve the integrity or functionality of the system. This may include the deletion of users' data.

If the RAD is notified of content on RAD-administered services that is in breach of the law or RAD Policy then the RAD will follow its procedures and will take all reasonable steps to remove or deny access to it.

Third-Party Access

The RAD's Internet connections are provided by Arrow/Gamma. It is not permitted to provide access for third parties without the prior agreement of IT to any IT Services.

Off-Site Access

Off-site access is provided for specific RAD IT services. Such services are limited for licensing or security reasons.

For information on remote access see the RAD Remote Access Policy.

Personal and Shared Data Storage

The RAD provides both personal and shared data storage for storing content for RAD-related work/study use. Examples of personal storage include the H:\ drive and cloud based storage like Synology and examples of shared data storage include the s:\, j:\ and i:\ drives.

RAD-provided personal storage should be used for storing RAD-related work/study content where only you require access to that content or for occasional, ad hoc sharing of that content with others. If you are sharing RAD-related work/study content with others on more than an occasional, ad hoc basis then appropriate RAD-provided shared data storage should be used instead. RAD data that is sensitive, personal, and confidential or of commercial value must only be stored on RAD-approved data storage.

Legal Compliance

It is the responsibility of each individual user to ensure that they do not break the law. Examples of the key areas of legislation are, but not limited to, the following:

i The Computer Misuse Act 1990 (amended by the Police and Justice Act 2006);

ii The Copyright, Designs and Patents Act 1988 and The Copyright (Computer Programs) Regulations 1992;

iii The Data Protection Act 1998;

iv The Defamation Act 1996;

v The Obscene Publications Act 1959;

vi The Criminal Justice and Immigration Act 2008;

vii The Communications Act 2003 and The Privacy and Electronic Communications (EC Directive) Regulations 2003;

viii The Equality Act 2010;

ix The Terrorism Act 2006;

xThe Regulation of Investigatory Powers Act 2000;

xi The Human Rights Act 1998;

xii The Counter-Terrorism and Security Act 2015

Policy Review

This policy will be reviewed by the Head of IT, Head of HR, and senior management team once a year from the date of issue.

Appendix A – Personal Use of RAD IT Services

The use of RAD IT Services for personal purposes must not:

i conflict with RAD Policy;

ii directly or indirectly interfere with the RAD's systems or burden the RAD with any incremental costs;

iii be for any personal, commercial or monetary gain;

iv conflict with the RAD's objectives or interests;

v conflict with an employee's obligations to the RAD as their employer;

vi be used for private confidential correspondence.

Subject to the above, occasional personal use of RAD IT services is allowed but it must not be excessive or interfere with one's duties, the work of others or other users' access to RAD IT services.

Examples of acceptable use are as follows:

i Occasional, limited, personal use of the RAD email or instant messaging systems. Such messages must be clearly marked as "Personal".

ii Recreational use of the Internet by an employee at agreed break times or outside their normal work hours.

iii Recreational use of the Internet on a RAD computer in the Student Computer Room during off-peak times when neighbouring computers are freely available for use by other users.

iv Storing non-work or non-study related content for access by yourself only on RAD IT services designated for your personal work or personal study use. Such storage must not be excessive in comparison to your stored work or study content, it must not infringe copyright or data privacy legislation and it must be stored under a folder marked “Personal”. The RAD cannot be held responsible for any loss to such content and it may be removed without prior notice if its storage contravenes RAD Policy. The user will be notified if this happens.

Appendix B – Unacceptable usage

RAD reserves the right to block, disconnect or otherwise prevent any usage of RAD IT services which it considers unacceptable. Unacceptable usage includes, but is not limited to, the examples given below. Please also see Appendix A for examples of unacceptable personal usage.

RAD IT services may not be used for any activity that may reasonably be regarded as unlawful or potentially so. This includes, but is not limited to, any of the following activities:

i creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;

ii creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety;

iii creation or transmission of material with the intent to defraud, including attempting to disguise the identity of the sender/origin of an electronic communication;

iv creation or transmission of defamatory material;

v creation or transmission of material such that this infringes the copyright of another person;

vi creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is authorised and relates to the academic or administrative activities of the RAD or is otherwise part of, a service to which the user has chosen to subscribe;

vii deliberate unauthorised access to networked facilities or services, including unauthorised access to unsecured or unattended network equipment;

viii deliberate or reckless activities having, with reasonably likelihood, any of the following characteristics:

a) Wasting colleagues’ effort or RAD IT resources, including time connected to accessible systems and the effort of others involved in the support of those systems;

b) Corrupting or destroying other users’ data;

c) Violating the privacy of other users;

d) Disrupting the work of other users;

e) Any form of denial of service attack;

f) continuing to use an item of software or hardware after it has requested that use cease because it is causing disruption to the correct functioning of RAD IT services or any connected network service;

g) the introduction of computer “viruses” or other harmful software or hardware, including, but not limited to, packet-sniffing and key loggers;

h) Unauthorised use of another user’s logon credentials;

i) Unauthorised network port or vulnerability scanning;

j) Unauthorised remote access of any equipment;

Examples of unacceptable activities or behaviours which adversely impact on the RAD include, but are not limited to, the following:

i committing the RAD to a contract unless officially authorised to do so;

ii any activities that compete with the RAD in business;

iii the creation or transmission of material that brings the RAD into disrepute;

iv the representation of any views and opinions held personally by the user as the views of the RAD, unless the user is explicitly authorised to do so;

v unauthorised transmission to a third party of confidential material concerning the activities of the RAD;

vi activities that unfairly criticise or misrepresent others;

Examples of unauthorised access to IT services include, but are not limited to, the following:

i allowing, inciting, encouraging or enabling others to gain or attempt to gain unauthorised access to the RAD’s IT services;

ii modifications to any RAD network, including the connection of networking hardware to the RAD network, made without the knowledge and authorisation of networking specialists within IT;

iii the registration of any domain name which includes the name of RAD or any similar name which may mislead users of that domain into believing the domain name refers to the RAD.