ROYAL ACADEMY OF DANCE

Information Security Policy

RAD Information Security Policy

1. Introduction

This Policy forms part of a suite of policies and procedures that support an information governance framework.

Recommended related IT policies:

RAD IT Acceptable Use Policy
RAD Password Policy
RAD Remote Access Policy
RAD Monitoring Policy
RAD Project Management Policy
RAD Email and Internet Policy
RAD Smartphone Usage Policy
RAD IT Equipment Disposal Policy
RAD Corporate Secure File Sharing Policy

2. Purpose

Information and information systems are valuable assets. Through policies, procedures and structures RAD strives to secure an uninterrupted flow of information, internally and externally. The RAD believes that information security is essential to ensure effective data sharing, and to support its academic and corporate objectives.

The following principle will be applied in the design and management of Information Security: Information, whether stored, in transit, or in use, is to be protected from unauthorised use and disclosure, thereby ensuring that confidentiality, integrity and accessibility are maintained.

3. Scope

This Policy applies to all information and Information Systems owned by the Royal Academy of Dance, including information and systems maintained by third parties on behalf of the Royal Academy of Dance. These include systems that are cloud based such as RADius, DanceBiz and others.

This policy applies to all employees, students and anyone else that uses RAD information systems or has access to RAD data.

4. Responsibilities

Governance
The Information Management Committee (IMC) ensures that security is properly evaluated and managed across the RAD. This Policy is sponsored by the IMC (Information Management Committee) of RAD. It is written and maintained under the direction of the Head of IT and is reviewed every 2 year(s). Appropriate members of the IMC will also ensure that all employees, students contractors and other third parties are advised when the policy is updated or amended.

Users
Users of RAD information systems and networks will act responsibly and in full compliance with all relevant policies and procedures when handling and sharing RAD information, in whatever format (i.e. digital or physical). Where sharing is in conjunction with third parties, appropriate sharing agreements will be in place.

Third Parties
Third parties, who manage, process, transmit or store information, or information systems on behalf of the RAD will act responsibly and in full compliance with this Policy and all relevant policies and procedures when handling and sharing RAD information.

5. Principles

Information is an essential asset that needs to be protected, especially in an increasingly interconnected communications environment. Information security measures protect information from a wide range of threats and safeguard based on the following security principles:

- **Confidentiality** – through protection from unauthorised access and disclosure.
- **Integrity** – by ensuring the accuracy and completeness of information and of processing methods.
- **Availability –** by ensuring that information and associated services are available to authorised users when required. Information exists in many forms and includes printed matter and electronic data, video, audio and text content.
- **Accountability:** by tracing actions and events back in time to the users, systems, and processes that performed them, to establish responsibility for actions or omissions.

Whatever form information takes and however it is shared or stored, all RAD information will be appropriately protected.

Lawful and appropriate management of systems and data is not only a corporate responsibility but also a personal one. Users will be held individually accountable for their own actions.

With reference to relevant Laws and Regulations the RAD will strive to ensure that:

- Systems and information comply with and are used within the framework of the law. This includes regulating access and monitoring communications.
- Information content remains lawful. This includes checking data and software across all RAD IT.
- Special care will be exercised in managing personal and commercially confidential data.

This Policy is brought to the attention of all new employees at Induction and to all new students and other users. It is the responsibility of employees, students and, all other users including contractors to remain up to date and routinely check the status of this Policy for updates and revisions, and other relevant RAD rules.

5. Behaviours

Risk assessment

Risk assessments should be performed to address the vulnerabilities of information content and systems and current threats. The RAD IMC can advise where appropriate on best practice.

Heads of Departments are responsible for ensuring effective risk management in their own areas. (Especially when sharing data with third parties or taking data off-site)

Business Continuity

Information security forms part of wider business continuity planning within the RAD. Information security requirements will be regularly and routinely reviewed and reassessed accordingly.

Physical and environmental security

Appropriate security measures will be installed and enforced to prevent unauthorised access, damage and interference with information and facilities.

To prevent loss, damage or compromise of assets and disruption to business activities, information and equipment will be protected as far as possible from environmental hazards both natural and man-made. This includes reasonable protection against power failures and the establishment and maintenance of an offsite alternative operating centre where justified and achievable

Security of information systems

Rules for accessing RAD information facilities, the responsibilities of users and the rights of the RAD are set out in the IT policies which all employees and students are required to comply with.
The following security measures are supported by the RAD to ensure the security of information and information systems:

- Strong Identity Management for users and information systems
- Proper Authorisation and Access Control for users and information systems.
- Appropriate encryption for information and subsequently the data in motion and at rest.
- Information and system backup and recovery. This includes cloud based systems and systems provided by third parties.
- Regular audit to ensure that only licensed and authorised software is used across IT in the RAD.
- Appropriate protection against malicious software and other forms of attack against IT in the RAD.

Users should recognise that inappropriate software interferes with the proper running of RAD systems and should not be installed or used.
Any authorised software should be used only within the terms of its licence and should be properly maintained and upgraded.
RAD information must remain secure when it is taken or viewed away from RAD premises this includes when working from home. Responsibility for data housed on mobile devices (notebooks, palmtops, laptops, smart cards, USB devices, digital pens, mobile phones and so on) rests with the user in control of the device. Users should take appropriate measures to secure both the data and the device.
The requirement for security of RAD information held outside the RAD applies equally to paper records and files.

Asset classification and control

To ensure effective asset protection the RAD will develop and maintain asset registers of hardware, software, systems and information.
All information and systems should be labelled by the information or system owner with relevant information classification.
Further details are available in the IT Information Assets.
A range of procedures and processes will be developed to support the systematic and secure handling of information assets across the RAD.
The RAD's Procedure for Security of Personal Information and the following main working practices should be implemented and monitored at a departmental level:

- Never leave sensitive or confidential documents unattended, or easily accessible
- Secure storage, including lockable filing cabinets and password protected computer files;
- Careful consideration about the best and most secure medium for communication and retention of sensitive information.

Requirements for retention and disposal of information

- Retention and disposal rules are addressed in the **RAD's Procedure for Records Retention and Disposal, Retention Schedule and Records Management Policy** (in progress) and other related documents. Appropriate procedures for information disposal should be made at a departmental level with support and guidance from the IMC as required.
- Confidential material (including personal data and commercially sensitive material) should be disposed of securely in accordance with the RAD's **Procedure for Security of Personal Information** and the **RAD IT Disposal Policy**.

- Physical records should be shredded or incinerated, digital data should be fully erased, under advice from RAD Information Technology (IT) staff and in accordance with the RAD's **Procedure for Security of Personal Information**.
- Backups should not be kept longer than required
- Backup Media such as tapes, hard drives and USBs etc. should be stored in a secure location, and where possible password protected or encrypted
- Where third parties hold data or provide systems, appropriate measures should be in place for data retention and disposal

Information security awareness

- Information security awareness is vital and the RAD will make efforts to ensure that users of information systems are informed and updated about best practice and current risks.
- All users of RAD information and information services (including contractors) will receive appropriate information about the security standards.
- Advice and support is available particularly for users with special responsibility for creating and managing information.
- Appropriate training will be provided including GDPR and Cyber Security Awareness.

6. Incident Reporting

Prompt reporting of security incidents is vital to minimise loss and damage. RAD reporting procedures are as follows:

- Refer to the **RAD Procedure for Information Security Incidents and Breach.** Physical security incidents (vandalism, theft and so on) or suspicious behaviour should be reported at once to Reception or Facilities.
- Physical software breaches (theft, overwriting, unauthorised access to data etc.) should be reported through the management chain of the relevant department.
- Information theft, manipulation or illegal access should be reported to the Head of IT or IT Service Desk. Mechanisms will be in place to monitor and quantify security incidents and to identify recurring breaches.

7. Enforcement

Failure to comply with this Policy or any related Policy might lead to appropriate disciplinary sanctions. Employees and students will be subject to the Employee or Student disciplinary procedure, which could lead to employees being dismissed or student studies being terminated. In some instances breach of this Policy may also be a breach of the law.

8. Review period

The Head of IT will review the policy every two years from date of issue.

9. Definitions

- RAD: Royal Academy of Dance
- IT: Information Technology
- IT service desk: 02073268030 rad.ict@rad.org.uk
- IMC : Information Management Committee (New name for Data Protection Committee)