

UK General Data Protection Regulation (UK GDPR) Accountability Statement

Effective Date: 24/06/21

The UK GDPR integrates accountability as a data protection principle in and requires organisations to demonstrate their compliance. This statement outlines the accountability of the Royal Academy of Dance (RAD) in relation to information management and protecting our members' and customers' privacy. Where the RAD will process personal data of European citizens, the accountability requirements of the EU GDPR will also be taken in consideration.

Management Structure and Governance

The Board of Trustees and Executive Board have delegated responsibility for data protection and records management to a dedicated Information Management Committee. This is chaired by the Director of Marketing & Communications (a member of the Executive Board) and membership consists of **Information Asset Owners** drawn from key departments across the organisation.

Supporting the committee is a group of Information Champions with responsibility for communication of and implementation of policy and procedures at an operational level. The Board of Trustees and Executive Board, via the Information Management Committee, remain accountable.

In addition, the Director of Finance and Operations has been appointed as **Senior Information Risk Owner** (formerly Data Controller) and the RAD and Royal Academy of Dance Enterprises Ltd. are registered with the Information Commissioner's Office (ICO). While the RAD has no legal obligation to appoint a **Data Protection Officer** we have appointed one on a part-time, fixed term basis, to support us in our compliance work and to provide independent oversight. More information about them can be found [here](#).

Lawful Bases for Processing Personal Data

The RAD has undertaken to identify and publish the lawful bases under which it processes personal information in all of the contexts in which it is collected and processed. We also hold a corporate retention schedule for all personal information held.

We acknowledge and abide by the supplementary legislation and regulations that govern processing, for example, Privacy & Electronic Communications Regulation (PECR) which governs the use of electronic communications in direct mail.

The RAD has identified the relevant and applicable lawful bases as documented on our website (<https://www.royalacademyofdance.org/privacy-policy/>) alongside our departmental privacy policies which can be found in the same link.

We work with our Data Protection Officer and other members of staff to ensure the correct lawful bases (and special conditions where applicable) are applied to our data processing activities as required under the UK (and EU) GDPR.

Privacy By Design

The RAD is committed to taking a 'Privacy by Design' approach. We have already created a Privacy Impact Assessment procedure and will continue to embed privacy consideration into our business practices and systems development, with advice from our Data Protection Officer.

Policies and Procedures

The RAD has created, revised and published a number of policies and procedures to ensure that we are able to comply with UK GDPR requirements:

- Information Management Policy and Procedures
- Procedure for authorised publication or disclosure of information
- Procedure for Information Security Incident
- Information Breach notification form
- Information Incident Risk Assessment form
- Information Incident or Breach risk matrix
- Procedure for Information Sharing (including an Information Sharing Agreement template)
- Procedure for Records Retention and Disposal
- Procedure for Right to Access Personal Information
- Subject Access Request Form
- Procedure for Rights to Erasure, Objection and Restriction
- Procedure for Security of Personal Information
- IT – Monitoring Policy
- IT – Information Security Policy
- Visual Media Policy (and associated documents)

Mitigation of Potential Risks

Organisational Measures

We are working with staff worldwide to raise awareness of the importance of privacy and information management, and to embed the data protection principles into our organisational practices. Staff at all levels have received training on data protection requirements and best practices. Committee members, champions and other key personnel have received more tailored training as it relates to their operational responsibilities, including cyber security. Refresher training is planned on a continuing basis, and an overview of data protection and introduction to RAD policies and procedures has been built in to the induction process for all new members of staff.

We include regular data protection and information management updates and guidance in our internal e-newsletter which aims to remind staff on privacy issues, highlights timely topics and trends, knowledge sharing and best practice across the organisation, and links to ICO news items and updates.

Our information security incident procedure and risk analysis ensures that we can assess an incident quickly and effectively so as to comply with the new 72-hour deadline for reporting serious breaches to the ICO and other supervisory authorities if required.

Technical and Organisational Security Measures

We are undertaking a risk analysis of our processing to enable us to put the appropriate security in place.

- We have created and implemented an information security policy and additional policies and procedures to underpin this.
- We have put in place some of the basic technical controls specified by the established Cyber Essentials frameworks. We will continue to assess what other technical measures may be required.
- When processing credit card payments we adhere to the PCI-DSS standards for securely processing personal data, and ensure that any third parties that we work with are also compliant.
- We use encryption or anonymisation where it is appropriate to do so and we ensure that any data processor we use also implements appropriate technical and organisational measures in accordance with the main services agreement or other data processor agreement/addendum.
- We will conduct regular testing and reviews of our measures to ensure they remain effective, and act on any areas highlighted for improvement.

Dated: June 2021

For Review: June 2012