GDPR Privacy Policy - Russell Maliphant Dance Company

Revised: 7 Jan 2020

ORGANISATION

Russell Maliphant Dance Company Ltd whose registered address is Jerwood House, 1-3 Foundry Lane, Ipswich, IP4 1DW

DATA CONTROLLER

Harry MacAuslan, Trustee - Russell Maliphant Dance Company Ltd

DATA PROCESSOR

Bella Scarr, General Manager - Russell Maliphant Dance Company Ltd

DEFINITIONS AND PURPOSES OF PROCESSING DATA

Data is processed for the following purposes:

MEMBERS OF STAFF:

- A paid member of staff at Russell Maliphant Company (salaried staff, tutor, dancer or contracter). The data is used to process salaries or payments, to contact the person or next of kin in emergencies, and to maintain contact details. Because Russell Maliphant Company undertakes classes and workshops for vulnerable people (children and young people, and persons with disabilities), a DBS check is carried out when appropriate.

VOLUNTEER/TRUSTEE:

- A volunteer or Trustee for Russell Maliphant Company. The data is used to contact the Volunteer regarding their work with us, to administer Trustee meetings and communicate with individual Trustees on relevant matters.

EDUCATION PARTICIPANTS:

- A student of Russell Maliphant Company (class member or workshop attendee) or a parent or guardian of (or nominated third party responsible for) a child/vulnerable adult attending a class or workshop. The data is used to process payment, contact with details about the class, or for emergencies.

PARTNERSHIP ORGANISATIONS:

- An organisation with which Russell Maliphant Company is engaged in providing educational services (e.g. classes and workshops) or a venue hosting a performance. The data is used to process payments and to contact them about the event.

EVENT ATTENDEES:

- An attendee of a Russell Maliphant Company performance (paid for performances, open rehearsals). Attendee data collected is used to administer the education activity; audience data will be collected by the Partnership Organisation under their own GDPR rules and shared with the Russell Maliphant Company in agreement with the Data Sharing Agreement included in all contracts/riders and signed by both parties prior to the event. The data is used to process payments, to advise the person should the event be cancelled or changed, and for monitoring purposes.

DONOR/GRANTOR:

- An organisation or person that supports Russell Maliphant Company via a financial or other contribution. The data is used to thank the donor for the contribution.

MARKETING PROSPECT/CONTACT:

- A person that has enrolled online to opt in to receiving the Russell Maliphant Company Newsletter (via Mailchimp). Person has asked to receive information about Russell Maliphant Company classes, workshops, education project and other related activities. The data is used to send information to that person/organisation.

RECIPIENTS OF PERSONAL DATA

Data Subject	**Recipient**
Member of Staff	Exec Producer, General Manager, Education Manager of Russell Maliphant Company
Volunteer/Trustee	Exec Producer, General Manager, Education Manager of Russell Maliphant Company
Education Participant	Exec Producer, General Manager, Education Manager of Russell Maliphant Company
Partnership Organisations	Exec Producer, General Manager, Education Manager of Russell Maliphant Company
Event Attendee	Exec Producer, General Manager, Education Manager of Russell Maliphant Company
Donor/Grantor	Exec Producer, General Manager, Education Manager of Russell Maliphant Company
Marketing Prospect	Exec Producer, General Manager, Education Manager of Russell Maliphant Company, and Mailchimp system for newsletter sign-up

TRANSFER OF DATA TO THIRD PARTIES

Russell Maliphant Company does not transfer any data to third parties except for software related to newsletters, surveys and bookings, such as Mailchimp, Event Bright or Survey Monkey.

RETENTION SCHEDULES

Russell Maliphant Company is undertaking a review of retention schedules for the data it holds. At present (May 2018), these are shown in the table below.

Data Subject	**Retention Schedule**
Members of Staff	Complete staff details are held for 7 years after leaving employment, in line with HMRC regulations, after which they are deleted. Details of name, role and terms of service are retained for the purposes of providing a reference.
Volunteer/Trustee	As per members of staff
Education Participant	Details held for 12 months from each enrolment to allow ease of booking. Data may include medical consent forms where appropriate. Data to be deleted on anniversary of last class attended.
Partnership Organisations	Data held for 7 years and reviewed each year
Event Attendees	Data is held for 12 months from the date of event and then deleted
Donors and Grantors	Data is held for 7 years from last donation, and then deleted
Marketing Prospect/Contacts	Following a GDPR mailchimp mailing sequence in May 2018 only contacts who opt in will be retained on these databases. Data submitted for the purposes of marketing lists will be deleted on request of the contact. New opt in subscribers' details will be retained until the subscriber requests to no longer receive communications

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES; LOCATION OF DATA; RECORDS OF CONSENT

The table below shows where data is currently stored and the measures in place to ensure it is safely stored.

Data Subject	Paper or Digital	Location
Members of Staff	Paper/digital	Locked filing cabinet; password protected computer
Volunteer/Trustee	Paper/digital	Locked filing cabinet; password protected computer
Education Participant	Paper/digital	Locked filing cabinet; password protected computer; company mobile
Partnership Organisations	Digital	Password protected computer
Event Attendee	Digital	Password protected computer
Donor/Grantor	Paper/Digital	Locked filing cabinet; password protected computer
Marketing Prospect	Digital – excel/Mailchimp	Password Protected computer

PRIVACY NOTICES PROVIDED TO THOSE SUPPLYING DATA

The Lawful Basis for processing

Member of Staff: The information you have supplied is only used in conjunction with your employment including: checking of references/DBS checks; payment of salaries/invoices; organising training. It is likely as a member of staff that you may attend classes, events and performances and data collected through those processes will be deemed subsidiary to your status as a member of staff which means, for example, that while data concerning attending a workshop may be deleted within 12 months, your employee data will be retained according to the guidelines by HMRC for data retention in regard to members of staff. (see also Marketing, below).
Lawful Basis: Consent

DBS Process: photocopies of relevant documents are taken and used for input into the online DBS system. Once entered, photocopies are shredded and a record of the DBS number and data of issue is kept on the staff member's file.
Lawful Basis: Consent

Volunteer/Trustee: The information you have supplied is only used in conjunction with engagement including: checking of references; organising training; contacting in the event of needed advice or guidance; organising Trustee meetings and functions. It is possible that a volunteer/trustee may attend classes or events in which case data collected through those processes will be deemed subsidiary to your status of volunteer/trustee. Therefore while data concerning event attendance may be deleted after 1 year, your volunteer/trustee contact data will be retained according to the guidelines for data retention. (see also Marketing, below).
Lawful Basis: Consent

Education Participant: The information you have supplied is only used in conjunction with attendance at your class/es including: processing of fees and contacting you in the event of changes (e.g. the venue being closed or a class being cancelled). (see also Marketing, below). Medical consent forms are completed where relevant and retained on the class file. Any financial details taken during a transaction are destroyed after the transaction and are not retained.
Lawful Basis: Consent

Partnership Organisations: The information you have supplied is only used in conjunction with the management of classes, workshops and events organised on behalf of your venue/charity/organisation. This includes: information about the event; processing of any fees; notifying you about any changes. (see also Marketing, below).
Lawful Basis: Consent

Event Attendee: The information you have supplied is only used in conjunction with the event attended, including: taking payment for the event and contacting you in the event of changes. (see also Marketing, below). For staff members and volunteers, please see the relevant sections above. Any financial details taken during a transaction are destroyed after the transaction and are not retained.
Lawful Basis: Consent

Donors and Grantors: The information you have supplied is only used in conjunction with communicating with you about your donation. This includes: discussing with you how your donation is used; financial details. We may refer to donations in our marketing and/or communications but only by way of an announcement, unless you have expressed anonymity. No contact details will be shared with any other party. (see also Marketing, below).
Lawful Basis: Consent

Marketing: Most of our communication materials (e.g. order forms, booking forms, purchasing forms etc) carry opt-ins to receive marketing material from Russell Maliphant Company. Legacy recipients of marketing material will be contacted about whether they still wish to receive these materials via an opt-in method. All details will be deleted if there has been no response to opt-in by 25 May 2018. Please note that this does not apply to personal details supplied in relation to class attendance or volunteering.

Lawful Basis: Consent

INDIVIDUALS' RIGHTS

Everyone whose details are kept by Russell Maliphant Company has the right to view any information retained by us. We will supply all such data in a digital file within 4 weeks of receiving such a request. The individual can ask for all their records to be deleted from our systems at any time. Such requests may affect the provision of services offered by Russell Maliphant to the individual but, to avoid confusion, such issues will be discussed with the individual before the information is deleted.

AUTOMATED DECISION-MAKING AND PROFILING

Russell Maliphant Company has no automated system for decision-making and profiling. The data kept is described above and is used either for the provision of services or the maintenance of essential contact (e.g. for members of staff).

Russell Maliphant Company uses Mailchimp for the delivery of its marketing emails. Mailchimp has some automated features but these are used only to analyse open and bounce rates of emails and are anonymous in their analysis.

SOURCES OF PERSONAL DATA

The table below shows how personal data is sourced:

Data Subject	**Data Type**	**Source**
Member of Staff	Paper/digital	Recruitment Process/Induction forms (including medical consent forms); DBS; opt-ins from paper/digital forms
Volunteer/Trustee	Paper/digital	Recruitment Process/Induction forms (including medical consent forms as appropriate); DBS as appropriate; opt-ins from paper/digital forms
Education Participant	Paper/digital	Class booking forms (including medical consent forms as appropriate)
Partnership Organisations	Paper/Digital	Contracts; Data sharing agreements

Event Attendee	Paper/digital	Booking form; opt-ins from paper/digital forms
Donor/Grantor	Paper/Digital	Donation form including opt-ins
Marketing Prospect	Digital – excel/Mailchimp	Opt-ins via website/forms

RECORDS OF CONSENT

Personal data is stored as above (see RECORDS OF CONSENT)

CONTROLLER-PROCESSOR CONTRACTS

Mailchimp terms and conditions of service: https://mailchimp.com/legal/privacy/

THE LOCATION OF PERSONAL DATA

Personal data is stored as above (see LOCATION OF DATA)

DATA PROTECTION IMPACT REPORTS

The table below highlights areas of risk in data protection

Data Subject	**Data location**	**RISK**
Member of Staff	Locked filing cabinet; password protected computer	**Medium**; filing cabinet needs to be kept securely locked. Protocols for Password Changes need to be introduced, particularly after staff changes
Volunteer/Trustee	Locked filing cabinet; password protected computer	**Medium**; filing cabinet needs to be kept securely locked. Protocols for Password Changes need to be introduced, particularly after staff changes
Education Participant	Locked filing cabinet; password protected computer; company mobile	**High**; limited security with relatively easy access to contact details, high risk data
Partnership Organisations	Locked filing cabinet; password	**Medium**; filing cabinet needs to be kept securely locked. Protocols for Password Changes need to be

	protected computer	introduced, particularly after staff changes
Event Attendee	Password protected computer	**Medium**; filing cabinet needs to be kept securely locked. Protocols for Password Changes need to be introduced, particularly after staff changes
Donors and Grantors	Locked filing cabinet; password protected computer	**Medium**; filing cabinet needs to be kept securely locked. Protocols for Password Changes need to be introduced, particularly after staff changes
Marketing Prospect	Password Protected computer	**Medium/Low** – but see recommendation under CONTROLLER/PROCESSOR CONTRACTS above.

RECORDS OF PERSONAL DATA BREACHES

To date (Jan 2020) there has not been a serious personal data breach.