RIVERSIDE DANCE'S DATA PROTECTION & GDPR POLICY

As a dance and performance company, Riverside Dance needs to gather and use certain information about individuals to enable it to carry out operations successfully.

These can include customers, suppliers, business contacts, past, present, and future supporters, employees, and other people the company has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled, and stored to meet the company's data protection standards – and to comply with the law.

Riverside Dance is committed to keeping personal information (data) safe and meeting our responsibilities under privacy and data protection law. This policy is intended to provide clear guidance for how Riverside Dance handles data. Our Privacy Policy outlines how we use data and individuals' rights in regard to this.

This policy refers to the current relevant legislation: the Data Protection Act ("the Act"), the General Data Protection Regulations ("the GDPR") and the Privacy and Electronic Communications Regulations ("PECR").

Why this policy exists

This data protection policy ensures Riverside Dance:

- Complies with data protection laws and follows good practice
- Protects the rights of staff, stakeholders, supporters, customers, and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Act and the GDPR describe how all companies – including Riverside Dance – must collect, handle, and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or in other ways.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR are underpinned by seven important principles. These are:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

PEOPLE, RISKS AND RESPONSIBILITIES

Policy scope

This policy applies to:

- All employees, workers, and volunteers of Riverside Dance
- All contractors, suppliers and other people working on behalf of Riverside Dance

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Act. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone number
- … plus, any other information relating to individuals

Data Protection risks

This policy helps to protect Riverside Dance from some data security risks, including:

- Breach of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- If customers feel their data is being used inappropriately or is at risk.
- Reputational damage, for instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Riverside Dance has responsibility for ensuring data is collected, stored, and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The Board of Trustees and Company Director are ultimately responsible for ensuring that Riverside Dance meets its legal obligations.

- The Data Protection Officer (DPO) – The Company Director - is responsible for:
    - Keeping the board updated about data protection responsibilities, risks, and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data Riverside Dance holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The Company Director is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

- The Communications team, is responsible for:
  - Approving any data protection statements attached to communications such as emails and letters.
  - Ensuring the storage of mailing lists is compliant with data protection rules.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Riverside Dance will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared. Additional two-step access should be set up where applicable.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the data protection officer or data controller.
When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to Riverside Dance unless the business can make use of it in accordance with an identified lawful basis for processing data. When using personal data, the following practices should be adhered to:

- Employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally.
- Data must be encrypted before being transferred electronically. The IT manager (Assured Digital Technologies) can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area unless there is reasonable certainty that country or territory also ensures an adequate level of protection.
- Employees should inform the DPO if they save copies of personal data onto their own computers. This data should be protected as per the data storage requirements above. Employees should always access and update the central copy of any data.

Data accuracy

The law requires Riverside Dance to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Riverside Dance will make it easy for data subjects to update the information Riverside Dance holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the Marketing team's responsibility to ensure marketing databases are checked against industry suppression files every six months.

Data review

Data management will be reviewed annually on a sample basis to ensure that it is accurate and being used, stored and in-line with this policy document.

Data breach response and notification

The following steps should be taken in event that a potential breach is discovered:

- The DPO should be notified immediately.
- The DPO will investigate to determine if there has been a breach under GDPR.
- If such a breach is determined to have happened the DPO will inform the relevant supervisory authority and affected data subjects within 72 hours.
- All breaches will be recorded in the Data Breach Log.

Subject access requests

All individuals, including employees, who are the subject of personal data held by Riverside Dance are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If a person contacts the company requesting their personal information, this is called a subject access request.

Subject access requests from individuals can be made by any means and the request could be communicated to any member of the company. The DPO can supply a standard request form, although individuals do not have to use this.

If an individual makes a subject access request and there is doubt concerning the identity of the person making a request the DPO may ask for more information, however they may only ask for information that is necessary to confirm their identity.

The DPO will aim to provide the relevant data within one calendar month. We reserve the right to charge a reasonable fee for requests that are manifestly unfounded, excessive or if an individual requests further copies of their data following a request.

The DPO will always appropriately verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Riverside Dance will disclose requested data. However, the DPO will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

Riverside Dance aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company. This is available on request and is also available on the company's website.