MID WALES DANCE ACADEMY

DATA PROTECTION POLICY

CONTEXT AND OVERVIEW

Introduction

Mid Wales Dance Academy needs to gather and use certain information about individuals. These can include donors, performers, volunteers, trustees, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to comply with the law.

Why this policy exists

This data protection policy ensures the organisation:

- Complies with data protection law and follows good practice
- Protects the rights of those whose data the organisation uses
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 2018 ("DPA") describes how organisations must collect, handle and store personal information.

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

The DPA is underpinned by certain principles. These require that personal data be:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is reasonably necessary
- handled in a way that ensures appropriate security, including protection against unauthorised access, save in accordance with a law enforcement request

PEOPLE, RISKS AND RESPONSIBILITIES

Policy scope

This policy applies to:

- All staff and volunteers of the organisation
- All contractors, suppliers and other people working on behalf of the organisation

It applies to all data that the organisation holds relating to identifiable individuals, including

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers

Data protection risks

This policy helps to protect the organisation from data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the organisation uses data relating to them.
- Reputational damage. For instance, the organisation could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with the organisation has some responsibility for ensuring data is collected, stored and handled appropriately.

The data protection officer, Lesley Walker, is responsible for:

- Keeping the trustees updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures annually.
- Handling data protection questions from anyone covered by this policy.
- Dealing with requests from individuals to see the data the organisation holds about them (also called ‘subject access requests’)
- Checking and approving any contracts or agreements with third parties that may involve the organisation’s sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Evaluating any third-party services the organisation is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with others to ensure marketing initiatives abide by data protection principles.

GENERAL GUIDELINES

- The only people able to access data covered by this policy should be those who need it for their role.
- Personal data should not be shared informally.
- Volunteers and employees should keep all data secure by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used.
- Personal data should not be disclosed to unauthorised people, either within the organisation 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 disposed of securely.
- Volunteers and employees should request help from 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.

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:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Volunteers and employees should make sure paper and printouts are not left where unauthorised people could see them.
- 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.
- If data is stored on devices these should be kept securely.
- Data should only be stored in safe restricted locations if saved online.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should never be saved to unsecured devices.

DATA USE

Personal data is of no value to the organisation unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, volunteers and employees should ensure the screens of their devices are locked if left unattended.
- Personal data may only be shared where the need arises and with consideration for the security of the data.
- Group email recipients should only be addressed in BCC / Blind Carbon Copy, unless it is clearly permissible to do otherwise.

DATA ACCURACY

The law requires the organisation to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort the organisation should put into ensuring its accuracy.

It is the responsibility of all volunteers and 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 reasonably possible. Staff should not create any unnecessary additional data sets.
- Staff should take every reasonable opportunity to ensure data is updated.
- Data should be updated as inaccuracies are discovered. For instance, a bounceback on an email address must be reported to the data protection officer who will follow up and update the primary data source.

SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by the organisation are entitled to:

- Ask what information the organisation 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 organisation is meeting its data protection obligations.

If an individual contacts the organisation requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data protection officer at info@mwda.co.uk

Individuals will be charged £10 per subject access request. The data protection officer will aim to provide the relevant data within 14 days.

The data protection officer will always verify the identity of anyone making a subject access request before handing over any information.

DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the DPA allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, the organisation will disclose requested data. However, the data protection officer will ensure the request is legitimate, seeking assistance from the trustees and from legal advisers where necessary.

PROVIDING INFORMATION

The organisation 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