# Cheshire Dance

# Data Management Policy

## 1. Context and overview

**Key details:**

- Policy prepared by: Debbie Cowley, General Manager
- Approved by board/management: November 2021
- Policy first became operational on: 25th May 2018
- Information Audit updated September 2021
- Next review date: October 2024

**Introduction:**

Cheshire Dance needs to gather and use certain information about individuals.

These can include artists, freelancers, workshop participants, board members, 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 meet the company's data protection standards – and to comply with the law.

**Why this policy exists:**

This data management policy ensures Cheshire Dance:

- Complies with data protection law and follows good practice
- Protects the rights of participants, staff, artists and partners
- Is transparent about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

**Data protection law:**

The General Data Protection Regulation (GDPR) applies in the UK and across the EU from May 2018. It requires personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals;
6. Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
7. The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

## 2. Who? People and responsibilities

Everyone at Cheshire Dance contributes to compliance with GDPR. Key officers understand the requirements and accountability of the organisation sufficiently to prioritise and support the implementation of compliance.

**Data Protection Officer (DPO) -** the person responsible for fulfilling the tasks of the DPO in respect of Cheshire Dance is:

Debbie Cowley, General Manager

The tasks of the DPO are:

- To inform and advise the organisation, the Board and its employees about their obligations to comply with the GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, advise on privacy impact assessments, conduct internal audits and support staff and freelancer training as part of in-house Safeguarding training.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, participants, trainees etc.)
- To issue Privacy notices to reflect lawful basis for fair processing, ensuring that intended uses are clearly articulated, and that data subjects understand how they can give or withdraw consent, or else otherwise exercise their rights in relation to the companies use of their data
- To ensure that audience development, marketing, fundraising and all other initiatives involving processing personal information and/or contacting individuals abide by the GDPR principles.
- To lead the Data Management Policy annual review

**Information and Communications Technology Officer** (ICTO) – the person responsible for IT systems and security compliance is:

Adam Holloway, Director

The relevant tasks of the ICTO are:

- To maintain secure ICT systems, performing tests and scans to ensure all systems, services and equipment used for storing data meet acceptable security standards.
- To manage internal data protection, data cleaning and updating activities and support internal auditing and staff training.
- To evaluate any third party services the company is considering using to store or process data, to ensure their compliance with obligations under the regulations

## 3. Scope of personal information to be processed

| **Cheshire Dance GDPR Information Audit** | **September 2021** | | | |
|---|---|---|---|---|
| **What personal data do we hold?** | **Where does the data come from?** | **Do we share this information, if so with whom?** | **Where is it stored** | **Security Measures** |
| **Class Participants** - Name, DOB, Address, phone number, email address, support requirements, ethnic origin, religion, gender, sexual orientation, emergency contact, image consent, safeguarding information | Registration forms | No | Dance Biz - Think Smart Software | Password protected |
| **Freelance artists / Trainees** - Name, address, phone number, email address, bank details, support requirements, ethnic origin, religion, emergency contact , gender, sexual orientation, DBS number, | Contract, Google Forms, Registration Forms | No | Drop Box<br>Bank details stored in Quick Books (Intuit) | Drop Box is Password Protected<br>Quick Books is Password Protected |
| **Staff** - Name , address, phone number, email address, DOB, bank details, National Insurance Number, P45, P60, payslips, pension, next of kin, support requirements, ethnic origin, religion, emergency contact , gender, sexual orientation | Contract, New starter form, email, Slade & Cooper, HMRC | Slade & Cooper - Accountants (Name, address, NI, DOB, P45, P60) | Encrypted backup data also stored off-site via industry standard Dropbox Business account.<br>Bank details stored in Quick Books (Intuit)<br>Main Office (Hard copy files)<br>Slade and Cooper Accountants (Iris Open Space, PAYE) | Iris - password protected, bank account password protected, email password protected<br>Hard copy files stored in locked filing cabinet<br>HMRC Checklist sent to new starters and forwarded to accountants. Data not stored on site |

| | | | | |
|---|---|---|---|---|
| **Board Members** - Name, address, DOB, phone number, ethnic origin, gender, occupation, nationality | Board Members | Charities Commission | Charity Commission | Charity Commission - password protected<br>Hard copy documents kept in locked filing cabinet |
| **Marketing Database -** email address, postal address and mobile number, communications preferences | Sign up via Mail Chimp (double confirmation) | Mailchimp<br>Other Arts Council England Funded Organisations by consent | Mailchimp (Web based) | Password Protected |
| **Business Contacts** - Name, title, organisation, address, email, telephone | Google searches, publicly accessible sources | No | TR Creative (ISP)<br>Encrypted backup data also stored off-site via industry standard Dropbox Business account. | TR Creative maintain industry standard data security Password Protected<br>Users (employees only) Password Protected<br>Windows security installed on workstations Router is firewall protected, password protected and uses WPA2-PSK security |
| **Stakeholders** - email addresses and correspondence | Stakeholders via email | Correspondents | TR Creative (ISP)<br>Encrypted backup data also stored off-site via industry standard Dropbox Business account. Workstations on LAN , Router | TR Creative maintain industry standard data security Password Protected<br>Users (employees only) Password Protected<br>Windows security installed on workstations Router is firewall protected, password protected and uses WPA2-PSK security |

## 4. Uses and conditions for processing

| Outcome/Use | Processing required | Data to be processed | Conditions for processing | Evidence for lawful basis |
|---|---|---|---|---|
| Regular Wildfire Newsletters and Updates | Campaign on MailChimp (GDPR compliant) | Email address<br>Postal address<br>Mobile number | Consent, with preferences user selected | Individual registration via Mailchimp. See statement below |
| Delivery of classes, workshops and residencies | Dance Biz Registration | Name, DOB, Address, phone number, email address, support requirements, ethnic origin, religion, emergency contact , gender, sexual orientation, safe guarding information | Consent, with preferences user selected | See statement below. |
| Payment of staff, artists, freelancers | Quick Books, Iris Open Space | Name, address, phone number, email address, DOB, bank details, National Insurance Number, P45, P60, payslips, pension, | Consent | See statement below. Signed and dated contracts |
| Companies House Register | Companies House online portal (new members registration) | Name, address, DOB, Occupation, Nationality | Consent | Board members co-opted at Board meetings |

**Consent and Privacy Notices**

**Contracts**

All contracts must be signed and dated before being returned to Cheshire Dance.

Wording used;

"Cheshire Dance will treat your data in accordance with GDPR regulations, store it securely and will not forward your information to other organisations. Cheshire Dance will use the information you provide on this form to be in touch with you and to safeguard your engagement with us. You can withdraw consent or request a copy of any information held or indeed request full data removal by emailing hello@cheshiredance.org or phoning the office on 01606 861770."

**Mailchimp**

To ensure that this is GDPR compliant Cheshire Dance is using the double opt in system that will evidence an affirmative action on behalf of the data subject and provide an audit trail to demonstrate how and when consent was obtained upon request.

Wording on MailChimp sign up form;

"We will treat your data in accordance with GDPR regulations and will not forward your information to other organisations without express permission. Cheshire Dance will use the information you provide on this form to be in touch with you and to provide updates and marketing. Please let us know all the ways you would like to hear from us:

- Email
- Text
- Post
- I am happy to receive marketing communications from other Arts Council England-funded organisations

You can change your mind at any time by clicking the unsubscribe link in the footer of any email you receive from us, or by contacting us at hello@cheshiredance.org. We will treat your information with respect. For more information about our privacy practices please visit our website. By clicking below, you agree that we may process your information in accordance with these terms."

**Dance Biz – NEW**

The following privacy statement requires a digital signature from anyone registering for classes on Dance Biz

"Cheshire Dance will treat your data in accordance with GDPR regulations, store it securely and will not forward your information to other organisations.

Cheshire Dance will use the information you provide on this form to be in touch with you and to safeguard your engagement with us.

You can withdraw consent or request a copy of any information held or indeed request full data removal by emailing hello@cheshiredance.org or phoning the office on 01606 861770"

## 5. Data Sharing

Arts Council England and National Portfolio Organisations

Via Mailchimp double opt-in sign up and through specific consent based on user selected communication preferences.

Mailchimp

Industry recognised, GDPR compliant list and email templates.

Slade and Cooper

Regulated by the Charity Commission, Financial Conduct Authority (FCA), Companies House, Homes and Communities Agency (HCA), HM Revenue & Customs (HMRC)

See consent statements in section 4

## 6. Security measures

Security Checks

- Cheshire Dance conducts enhanced DBS security checks on all staff who have access to children and vulnerable adults through the organisation's activities and services. Checks are repeated every 3 years.

Staff Training

- Staff training is conducted on 2 levels :-
  - Data Privacy training for practitoners (staff, freelancers and visiting artists) which forms part of Cheshire Dance's obligatory safeguarding training. It includes content on personal data protection and use of social media (This training is updated regularly as it is also bought in by other organisations)

  - Core staff training – those who access the Main Office Server and who are responsible for line managing others who access private data. These are programmed during regular staff training days. Security updates can be issued at any times or given at staff meetings.

Hard Copy Data

- Locked filing cabinet in locked Office
- Alarmed Building (Cheshire West and Chester Council tenant)

Workstations on LAN, Router

- Users (employees only) are Password Protected
- Windows security installed on workstations
- Router is firewall protected, password protected and uses WPA2-PSK security

Backup Data

- Encrypted backup data also stored off-site via industry standard Dropbox Business account.

Safe Transfer of Data

- Only those staff and freelancers can access personal information to ensure the safe engagement with participants, artists, trainees
- Arts Council England and National Portfolio Organisations - Data-sharing is not presently used. If it is in future, all data sharing will be subject to specifically negotiated data sharing agreements with access to personal information limited to the consent given and to specifically named personnel.
- Use of Egress email software for secure transfer of personal data used by specific agreement with funding bodies (i.e. Local Authorities, Arts Council England)

Password Management

- User passwords are not shared, nor written down.
- Passwords for external website profiles are stored in a password protected word file and stored off-line. The policy surrounding this password is the same as for user passwords.

Deleting Data and Decommissioning Hardware

- Hard copy personal data is shredded when we are no longer obliged to store it by law. Confidential data is cross-shredded.
- Personal data stored digitally by Cheshire Dance is stored on a range of industry standard cloud tools - Dropbox, Quickbooks Online, DanceBiz, TRCreative (website/email)

Privacy Impact Assessments (PIAs)

- DPIAs are undertaken for new projects where to potential risk of data breach is high. The purpose is to identify and fix problems at an early stage, reducing the associated costs and damage to individuals / organisational reputation which might otherwise occur. The PIA should contain:
  - A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
  - An assessment of the necessity and proportionality of the processing in relation to the purpose.
  - An assessment of the risks to individuals.
  - The measures in place to address risk, including security and to demonstrate that you comply.
  - A DPIA can address more than one project.

## 7. Data Breach

A personal data breach is:

- "A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service".
- A personal data breach may mean that someone other than the data controller gets unauthorised access to personal data. But a personal data breach can also occur if there is unauthorised access within an organisation, or if a data controller's own employee accidentally alters or deletes personal data.

How we know if a data breach has taken place?

- By notification via stakeholders. Encourage all stakeholders to notify the organisation of a suspected data breach
- By monitoring user access to the Main Office Server
- By ensuring third parties who hold personal data to notify us in accordance with GDPR regulations

Examples of a data breach

- Participant contact details, images, whereabouts known at specific times. Could lead to for example house break-in, victim profiling of vulnerable adults/young people.
- Marketing contact details lost to 3rd parties. Could lead to spam advertising.

Action (DPO lead)

- Report breach to the DPO / Director
- Risk Assessment (Conducted by DPO)
  - Personal, compliance, organisational risks
  - Likelihood, severity, score, reporting decision (If 'very high' inform ICO/Police)
- Record details in a breach log – facts, effects and remedial action
- Report the data breach directly to the Chair, to the commissioning/funding body and to those effected, describing a summary of the incident, when and what data has been unlawfully accessed along with a risk assessment / actions
- Measures taken/to be taken to recover/delete data and minimise negative impact of high/medium risks
- Actions individuals / organisations can take to mitigate possible adverse impact.

## 8. Social Media and Privacy

See Appendix 1

## 9. Automated processing

Cheshire Dance does not perform any automated processing, nor append information via external datasets.

## 10. Subject access requests

All individuals who are the subject of data held by Cheshire 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

Cheshire Dance will fulfil subject access requests in timely manner. When a subject access request is received by the DPO from an individual this will be actioned at the earliest opportunity and the individual will be notified by email of action taken to fulfil this request.

## 11. The right to be forgotten

Cheshire Dance respects the individual's right to be forgotten. When Cheshire Dance receives a request from an individual for their information to be deleted from our database all information will be removed and none of this information will be retained anonymously. This is mainly relevant to our Mailchimp list for marketing activities, where the user is able notified of their right to update their profile or unsubscribe in all direct email communications and at any time.

## 12. Privacy notices

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

- Who is processing their data
- What data is involved
- The purpose for processing that data
- The outcomes of data processing
- How to exercise their rights.

Privacy notices are provided at source, where information is first recorded as specified in section 3.

## 13. Review

Cheshire Dance will review this policy whenever any changes occur to personnel, practices or policies, or technical infrastructure that impact any of the information given. A formal date for holistic review is given in section 1, but the document is considered to be a dynamic articulation of the organisations data management policy which is under constant revision.

## Appendix 1

**Social Media and Privacy**

**Benefits of engaging with social media**

Social media provides a range of unique opportunities for dance artists and organisations. It can help us:

- Promote the benefits of our services to all children, young people and vulnerable adults and it can be a route to the hard-to-reach groups/ rural locations
- Engage, connect and develop unique interaction with people in a creative and dynamic medium where users are active participants
- Disseminate messages about events or campaigns virally among supporters in online communities
- Be a space for dance making and performance
- We must balance the benefits of creativity, spontaneity and immediacy of the communication with the potential risks, including the risks to children.

**Good practice guidelines as practitioners and dance organisations:**

**Planning your social media strategy**

- Think about your objectives
- Review your existing safeguarding policies and procedures
- Decide who will manage your social media
- Get to know the service you want to use
- Integrate online safeguarding into your existing safeguarding strategy

**Setting up your social networking page**

- Use an official organisation email address
- Keep your log-in details secure
- Set the appropriate privacy levels
- Set the 'accept comment' setting so you can check messages
- Include details so people can contact you directly
- Promote your social networking page on your website
- Register as a charitable organisation with your service provider - if appropriate

**Promoting safety online**

- Don't target underage children
- Don't accept 'friend' requests from underage children
- Avoid taking personal details of children, young people and vulnerable adults
- Be careful how you use images of children, young people or vulnerable adults
- Remind people to protect their privacy online
- Think before you post
- Promote safe and responsible social networking & provide links to safety and support organisations
- Data Protection considerations
- Beware of fake celebrity or dance profiles

**Safeguarding yourself - personal use of social networking sites**

Be aware of the impact of personal social media use upon your professional standing. In practice anything posted on the internet will be there forever and is no longer in your control. When something is on the internet even if you remove it, it may have already been "snapshotted" by a "web crawler" and so will always be there. Current and future employers and service users may see this. Keep all professional work completely separate from your private life.

**Safeguarding yourself, staff and vulnerable groups**

- Think about your privacy settings - 'just friends' means that your details, comments, photographs can only be seen your invited friends. However, always remember anyone who can access your site can potentially copy and paste your comment into the public domain making it visible to all
- Do not post embarrassing material or comments that may call into question your employment status
- Do not accept friendship requests on social networking or messaging sites from students, pupils, young people (or their parents) or vulnerable adult service users that you work with. For those working with young people remember that ex pupils may still have friends that you may have contact with through your work with the organisation
- Do not accept friendship requests unless you know the person or want to accept them – be prepared that you may be bombarded with friendship requests from people you do not know
- Choose your social networking friends carefully and ask about their privacy controls
- Exercise caution, for example, on Facebook if you write on a friends "wall" all of their friends can see your comment even if they are not your friend
- There is a separate privacy setting for Facebook groups and networks. You may have your own profile set to private, however, when joining a group or a network please be aware that everyone in that group or network are able to see your profile
- If you have younger friends or family members on your social networking groups who are friends with students, pupils, young people (or their parents) or service users that you work with, be aware that posts that you write will be visible to them
- Do not use your personal profile in any way for official business. If you are going to be a friend of your organisations official social networking group ensure you have a separate professional profile and do not use your personal profile
- Do not use your work contact details (email or telephone) as part of your personal profile.