Data Protection and Confidentiality Policy

REVIEW DATE: June 2025

SECTION 1: INTRODUCTION

Dublin Youth Dance Company (DYDC) recognises its responsibility in managing and processing personal data, sensitive personal data as well as other sensitive information that does not fall under the category of personal data. This policy outlines DYDC's approach to Data Protection and Confidentiality in the management of personal data and other sensitive information.

DYDC recognises that a guarantee of confidentiality is an important factor in determining the level of trust its members, their parents/guardians, as well as our staff and volunteers have in the company. We are committed to handling personal data and confidential information in a manner that is respectful, purposeful, professional and meets statutory requirements.

1.1 Data Controller

Dublin Youth Dance Company is the Data Controller under the definition provided by the GDPR. The person responsible for ensuring that the company meets its data protection responsibilities is Mariam Ribón (Artistic Director). Any queries or requests relating to personal data should be referred to this person.

Mariam Ribón (Artistic Director)
Email: dydcdirector@gmail.com
Telephone: 086 863 9702

1.2 Definitions

Personal Data: any information relating to an identified or identifiable natural person. Examples include name, address, contact details, age, date of birth. Personal Data can also refer to a photographic or video image of an identifiable person.

Sensitive Personal Data: special categories of personal data, which include health data, biometric data, genetic data, sexual orientation and religious beliefs.

Other Confidential Information**:** sensitive information that cannot be categorised as Personal Data but that, in the context of DYDC, is provided in the expectation that it will be properly managed. Examples include welfare/child protection reports, disciplinary reports.

Data Subject**:** an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier.

Data Processing: any operation or set of operations performed on personal data or a set of personal data. You do not need to view the actual data, but transmitting it, backing up a file or destroying data all count as a processing activity, even where the data is encrypted. Data processing can be both automated and manual.

Data Controller: a person or organisation that determines the purposes and means of collecting and/or processing of personal data.

Data Processor: a person or organisation that processes personal data on behalf of the Data Controller.

SECTION 2: DATA PROTECTION POLICY

In order to conduct its legitimate activities DYDC must collect and process categories of personal data, sensitive personal data and other confidential information. The following information is held by the company and should be treated as confidential.

- Staff, teacher and volunteer records, including application forms that contain personal data, details of any disciplinary action, etc.
- Garda Vetting Information including garda vetting application disclosures.
- Member Information/Parental Consent Forms that include details such as date of birth, information on medical conditions, etc.
- Welfare/Child Protection Reports.
- Contact information for stakeholders, supporters, etc.
- Marketing information such as the names and contact details of audience members, individual donors and supporters.

DYDC is aware of the Data Protection Acts (1998/2003 and subsequent amendments) and Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR). These Acts and Regulation govern all aspects of the treatment of personal data and sensitive personal data. We are committed to the following seven principles contained in Article 5 of the GDPR which regulate the processing of personal data:

1. **Process personal data lawfully, fairly and transparently:** We base our data processing on one or more Lawful Processing Conditions provided for by the GDPR. In the majority of instances, we will base our processing of Personal Data on the Consent of the Data Subject (Article 6, GDPR) and Sensitive Personal Data on the Explicit Consent of the Data Subject (Article 9, GDPR).

2. **Specified and Lawful Purpose:** We keep personal data only for one or more specified and lawful purposes and process it only in ways compatible with the purposes for which it was initially given.

3. **Minimisation of Processing:** Our processing of personal data will be adequate, relevant and restricted to what is necessary in relation to the purposes for which it is processed.
4. **Accuracy:** We keep personal data accurate and up to date.
5. **Storage Limitation:** We retain it no longer than is necessary for the specified purpose or purposes.
6. **Security and Confidentiality:** We keep personal data safe and secure.
7. **Liability and Accountability:** We will ensure personal data is processed in compliance with the GDPR.

2.1 Data Subject Rights

In managing and processing personal data, DYDC upholds the rights of the Data Subject as provided under the GDPR including:

- The right to be informed about how we will use their personal data.
- The right of access to a copy of the personal data we hold and information on how we process it.
- The right to have incorrect or incomplete personal data corrected.
- The right to be forgotten and have personal data deleted if they so request.
- The right to restrict how we process their personal data.
- The right to object to the processing of their personal data.
- The right to data portability.

2.2 Consent and Transparency

In the majority of cases, consent is the lawful grounds on which we process personal data. We will only process data where consent is affirmative, freely given, specific, informed and unambiguous. Consent will be sought from all data subjects using manual and digital forms as appropriate.

At the point of collecting data, data subjects will also be provided with a Privacy Statement (included in Consent Forms) detailing how and for what purpose the data will be processed. This will include the following:

- the identity of the Data Controller (and contact details for data requests),
- the purpose of collection,
- whether any sharing with third parties will take place,
- how long the data will be held,
- the details of the individual's rights regarding the data,
- notice of any automated decision-making ('profiling') that may take place using the data.

2.3 Processing Children's Data

In the context of youth dance, it is necessary to process the personal data of children.

- For all children aged under 18 who are engaged in DYDC activities, we will seek consent from the child's parent/guardian.
- In line with the requirements of the GDPR we will verify the child's age through confirmation by the parent.
- Also in line with the GDPR, we will verify parent/guardian consent via our Parental Consent in the company members agreement (see Child Protection Policy).

2.4 Third Party Data Processors

From time-to-time DYDC will need to engage third parties to process personal data on our behalf as necessitated by the nature of the processing. This will be notified to the Data Subject at the point of seeking consent for use of personal data. DYDC exercises reasonable care to ensure that the Data Processor carries out the processing in strict compliance with the GDPR, including ensuring that GDPR compliant agreements exist between DYDC and the data processor in respect of the processing.

Third parties that currently process data on our behalf include:

- Wix (email newsletters)
- Survey Monkey (survey data)
- Social Media
- DYDC website developer

SECTION 3: DATA SECURITY POLICY

3.1 Who has access to personal data and confidential information?

The following have access to personal data and confidential information through their involvement with DYDC:

- Designated Liaison Person
- Deputy Designated Liaison Person
- Teachers/Tutors

Personal data and confidential information as defined above is stored on company-owned laptops and private computers, company-owned external hard drives and in secure "cloud-based" storage systems. Due to the fact that DYDC does not have a dedicated office space, a small number of physical files are also kept by the Artistic Director in her private residence. Digital data is stored securely and protected by anti-virus software.

DYDC requires that all those who have access to personal data / confidential information because of their involvement with the organisation, adhere to the following:

- Be aware of the sensitive nature of the information to which you are privy and recognise the responsibility you have as a result of having access to this information.
- Familiarise yourself with our data protection and confidentiality policy and act accordingly.

- Be aware that information including written reports is the property of DYDC.
- Use personal data and confidential information only for the purpose(s) for which it was provided and the purpose(s) for which you are authorised to use it.
- Do not pass personal data on to third parties without the consent of the person in question.
- Do not share confidential information or pass it on to a third party unless it is absolutely necessary as in the case of a child protection concern. Making a child protection report is not a breach of confidentiality.
- All computers containing company information should have a log-on password.
- Robust security passwords should be used for all confidential files.
- Hard copy files/computer files should be retained and destroyed/deleted in line with DYDC's retention policy (see Section 4)
- Be aware that personal data and confidential information may also be contained on other media such as audio or video files.
- Staff/teachers may receive information that is confidential in error as in the case of an overheard conversation. Any information gained in this fashion is subject to the same conditions as information gained in an authorised manner and should not be shared.
- Staff/teachers should be particularly careful when they are in possession of sensitive personal data / confidential sensitive information in the workshop space or in a public space.
- The requirement of confidentiality continues to apply after an individual's involvement with DYDC ends.
- DYDC is aware of the particularly sensitive nature of garda vetting disclosures and records of child protection concerns. Should the Designated Liaison Person cease engagement with the company or no longer carry out this role, any garda vetting disclosures/child protection reports should be passed on to the Chairperson. They will then be given to the new Designated Liaison Person (DLP).
- As already stated, under no circumstances will garda vetting disclosures be shared with third parties.
- Where a disclosure has been returned outlining convictions or specified information, the identity of the applicant will be shared on a need-to-know basis. The DLP and the Chairperson will be aware of the identity of the applicant. Other members of the relevant decision-making committee will be given relevant information in relation to the disclosure but will only be informed of the identity if this is necessary or unavoidable.

3.2 Data Access Requests

Any Data Subject can make a Data Access Request and should direct the request via the individual responsible for overseeing Data Protection as detailed above. DYDC will observe the following when handling such requests:

- We will request valid proof of identification from the individual before proceeding with the request.
- If requested, access to a copy of their data will be provided in electronic form with details of how it is processed, within one month.
- Any corrections requested will be made within one month.
- If requested, we will delete a data subject's data within one month unless there is a valid reason not to (e.g. Garda Vetting Disclosures)
- We will halt processing on disputed data immediately until the issue is resolved.
- We will provide data in a digital format to a third party on the written request of the data subject. We will do this within one month.

3.3 Breaches of Data Protection and Confidentiality

- A breach of confidentiality may lead to a disciplinary procedure.
- In cases of a data breach, DYDC will make a report to the Office of the Data Protection Commissioner no later than 72 hours from becoming aware of the breach.

SECTION 4: Data Retention Policy

DYDC has developed the following retention policy stating the retention periods for the various types of information it holds. After the stated period has elapsed the information will be deleted from computers and any hard copy files will be shredded.

If there are any outstanding issues relating to any area of DYDC's work, the period of retention for any documentation related to this issue will only commence once the issue is satisfactorily resolved.

Description of Data (non-exhaustive examples)	**Retention Period**
Financial documentation including end of year accounts, other financial statements, invoices, receipts…	6 years
Records of **DYDC activities** including production images, programmes…	Permanent
Strategic plans, programme plans…	Permanent
Recruitment Records including unsuccessful applications, written record of interview panel's recommendations…	1 Year
Personnel Records including applications and CVs of successful candidates, references, contracts, training records, resignation and retirement letters, annual leave records, sick leave records, compassionate leave records…	6 years from the end of contract

Disciplinary Records	1 Year
Details of Grievance Procedures *(In cases of more serious disciplinary/grievance procedures or where an allegation of abuse is made against an employee, the records can be kept permanently)*.	6 months
Members' Personal Details	Throughout membership and participation plus 2 years after leaving.
Records of Complaints Procedures	5 years
Welfare Reports/Child Protection Reports	Permanent
Garda Vetting Information including disclosures	Proof of identity and garda vetting disclosures for staff will be retained throughout their involvement in DYDC. If they are re-vetted, the existing records will be replaced with new information/disclosure. When staff involvement finishes, we will retain their garda vetting records for 1 year from the finish date.