Dance United Yorkshire (DUY)

Our Data Protection Policy

1. The aims of this policy

In order for DUY to function effectively, from paying salaries and bills to agreeing contracts and maintaining contact with our service users, it is obviously necessary for us to collect and use certain personal information about particular individuals. These can include clients, partners, employees, volunteers, suppliers, business contacts and others with whom the charity has a relationship or may have reason to contact.

We aim to ensure that all such personal data collected about staff, service users, parents/carers, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

The DUY policy set out in this document applies to all personal data, regardless of whether it is in paper or electronic format. "Personal Data" means data which relates to a living individual who can be identified from either:

(a) the data, or
(b) the data and other information which is in, or is likely to come into, the possession of the data controller. This includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person, in respect of the individual.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. In addition, this policy complies with our funding agreements and articles of association. It aims to comply with any other relevant guidance from relevant sources e.g. the Charity Commission.

3. Definitions

Various terms used in this policy have specific meanings and these are explained in the following table:

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

DUY is a data controller as it processes personal data relating to service users, parents/carers, staff, trustees, visitors and others.

5. Roles and responsibilities

This policy applies to all staff employed by DUY, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 The Board of Trustees
The Trustees have overall responsibility for ensuring that DUY complies with all relevant data protection obligations.

5.2 Data Protection Officer
The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Board of Trustees and, where relevant, advise the board and make recommendations on data protection issues.

The DPO is also the first point of contact for individuals whose data the DUY processes. Our General Manager is the DPO for DUY. Currently this is Duncan Bedson and he is contactable via duncan@duy.org.uk.

5.3 All staff
DUY staff members are responsible for:

- Acting in accordance with this policy when collecting, storing and processing any personal data
- Informing DUY of any changes to their personal data, such as a change of address
- Contacting the DPO if they:
    - have any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - have any concerns that this policy is not being followed
    - are unsure whether or not they have a lawful basis to use personal data in a particular way
    - need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - believe or suspect there has been a data breach
    - are engaging in a new activity that may affect the privacy rights of individuals
    - need help with any contracts or sharing personal data with third parties

6. Data Protection Principles

The GDPR is based on data protection principles with which DUY must comply.

These principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes only
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how DUY aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one or more of the six 'lawful bases' (legal reasons) to do so under data protection law i.e.

- The data needs to be processed so that the DUY can fulfil a contract with the individual, or the individual has asked DUY to take specific steps before entering into a contract
- The data needs to be processed so that DUY can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the DUY can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of DUY or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a young person) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services, such as Zoom dance sessions, and we intend to rely on consent as a basis for processing, we will get parental consent where the young person is under 13 (except for online counselling and preventive services).

When we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a service user or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies, and we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and service users e.g. IT companies. When doing this, we will:
    - Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies in circumstances where we are legally required to do so, including:

- Prevention or detection of crime and/or fraud
- Apprehension or prosecution of offenders
- Assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them respond to an emergency situation that affects any of our service users or staff.

If we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information held by DUY about them. This includes:

- Confirmation that their personal data is being processed

- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- With whom the data has been, or will be, shared
- For how long the data will be stored or, if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual him/herself
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

Any subject access request received must be immediately forwarded to the DPO.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of child aged 12 and above at DUY may not be granted without the express permission of that child. This is not a fixed rule as a child's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge

- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the individual
- Would reveal that the individual is at risk of abuse, where the disclosure of that information would not be in the individual's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the individual.

We may refuse to act on a request if it is unfounded or excessive, or charge a reasonable fee which takes into account administrative costs. A request will be considered unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why and explain that they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive an explanation when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format

Individuals should submit any request to exercise these rights to the DPO. If other members of staff receive such a request, they must immediately forward it to the DPO.

10. Biometric Recognition Systems

Currently not applicable.

11. CCTV

Currently not applicable.

12. Photographs and videos

As part of our DUY activities, we may take photographs and record images of individuals within our programme of work. We will obtain written consent from parents/carers, or participants aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials. Where we need parental consent, we will clearly explain how the photograph and/or video will be used, to both the parent/carer and student. Where we do not need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Uses may include:

- DUY brochures, newsletters, etc.
- Outside of DUY by external agencies such as the local/national media outlets
- Online on DUY's website and/or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way, we will not accompany them with any other personal information about the participant, to ensure they cannot be identified.

13. Data protection by design and default

We have measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably skilled DPO, and ensuring that this person has the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)

- Completing privacy impact assessments where DUY's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the main office
- Passwords that are at least 6 characters long are used to access DUY computers, laptops and other electronic devices. All devices will be subject to automatic lockout if not being used.
- Encryption software is in place for all laptops and work phones.
- Staff or Trustees who store personal information on their personal devices are expected to follow the same security procedures as for DUY owned equipment.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely and in a timely manner. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on DUY's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

DUY will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person
- The theft of a DUY laptop containing non-encrypted personal data.

17. Training

All staff and Trustees are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or DUY's processes make it necessary.

18. Monitoring arrangements and links with other policies

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed and updated at least every 2 years and shared with the Board of Trustees.

This data protection policy is linked to our:

- Safeguarding Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO

- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people

- The DPO will alert the Chair of Trustees.

- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

- The DPO will determine whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identity theft or fraud
    - Financial loss
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned
    - If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

  - The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
  - If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  The DPO and Chair of Trustees will meet as soon as is reasonably possible to review the circumstances and decide how to prevent such a breach occurring in the future.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records):

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public. If it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- The DPO will contact relevant authorities (e.g. the police, software companies, companies who process data on DUY's behalf) to attempt to retrieve the information or delete it. The DPO will contact the ICO and individual(s) affected.

A DUY laptop containing non-encrypted sensitive personal data being stolen or hacked:

- The DPO will contact relevant authorities (e.g. the police, software companies etc.) to attempt to retrieve the information or delete it
- The DPO will contact the ICO and individual(s) affected.

Paper records of sensitive information being lost or stolen:

- The DPO will contact the ICO and individual(s) affected.