# Privacy, Data Protection and Information Security Policy

**Updates:**

- Reviewed wording and content
- Nothing to update since 2024

| | |
|---|---|
| **Previous Update** | Feb 2024 |
| **Current Update** | Feb 2026 |
| **Next Update** | Feb 2027 |
| **Review Cycle** | Annual |
| **Lead Contact** | Sanjay Dasani, Head of Operations |
| **Approval by** | Audit Committee (via Rep) |

# Privacy, Data Protection and Information Security Policy

## Policy Statement

In the management of confidential information the Contemporary Dance Trust Ltd (trading as The Place) will operate in a way that fully embraces the principles of privacy, transparency and equality. As a minimum requirement we will ensure the warranted and legal collection and use of information and actively prevent its unauthorised access, misuse or loss. We will also set ourselves a standard which exceeds that stipulated by law and be an exemplar for others to follow. We will communicate this policy and associated procedures in a simple and effective manner to everyone granted access to information systems to ensure awareness.

## Scope

This policy covers all information collected and used by The Place, access to which is subject to restriction whether stored on paper or in electronic formats. This is referred to as Confidential Information throughout this policy and for The Place this specifically refers to:

- Personal information – access restricted by the General Data Protection Regulations 2018 (GDPR) and the Privacy and Electronic Communications Regulations (PECR)
- Sensitive data as defined by the GDPR
- Payment card data – access restricted by the Payment Card Industry Data Security Standard (PCI DSS)
- Commercially or legally sensitive information
- Bank details.

It applies to anyone granted access to The Place information systems who thereby has a duty to adhere to this Policy and related procedures. All employees will be required to sign the declaration at the bottom of this document to confirm acceptance as part of induction. In addition, employees will be required to attend or undertake IT Data Protection & Security training or e-learning within one month of joining.

## Roles and responsibilities

The Place is registered with the Information Commissioner's Office (ICO) as a Data Controller. The lead Data Protection Officer and primary point of contact for both data subjects and the Information Commissioner is the Head of Operations.

Heads of Department (The Place Directors) are responsible for ensuring policies and practices are properly implemented on a day-to-day basis, and ensuring that all staff, contractors and freelance artists are properly aware of the policy and its implications for their involvement with the organisation.

All members of The Place staff, including freelancers working on fixed-term contracts, have an individual responsibility for ensuring the personal implementation of the Privacy, Data Protection and Information Security policy in their work with The Place

**Principles**

- **Access**. We only grant access to confidential information on a need-to-know basis and for as long as is required. Individuals requiring access will first have to agree to the terms of this Policy. Third party organisations requiring access will have to sign a confidentiality agreement. We actively monitor access and reserve the right to restrict access at any time.
- **Data Collection**. We only collect confidential information and in particular personal information that is deemed necessary to conduct The Place business and that is covered by our data protection notification to the Information Commissioner's Office.
- **Secure Storage, Data Accuracy and Retention**. We store all confidential information securely. We actively manage and maintain the security of this data according to the relevant standards. We ensure that confidential information is kept up to date and ensure secure disposal when it is no longer required.
- **Secure Transfer**. We ensure the security of confidential information when it is in transit beyond the controls of our secure network (e.g. through encrypted removable media).
- **Transparency**. We maintain a Privacy Policy on our website that clearly explains our collection and use of personal information. We ensure our customer service team can explain and respond to or escalate public enquiries in relation to the Privacy Policy with clarity and efficiency. We specifically maintain a procedure that makes it possible to efficiently respond to Subject Access Requests within the timescales defined by the GDPR and we monitor our ability to do so.
- **Who we contact**. We only ever contact people who have asked to be contacted by us or where it is reasonable or a specific requirement to do so. If we get this wrong, we quickly put in place measures to address this error.
- **Procedures**. We maintain a set of detailed procedures that cover all The Place activities that relate to the processing of confidential information.
- **Training and support**. We endeavour to ensure thorough understanding for anyone at The Place who directly handles confidential information through training and support.
- **Governance**. The Audit Committee is tasked with periodically reviewing this Policy as part of its annual work plan, to ensure the ongoing effective implementation of the policy, to identify any changes to business practice that may require policy or procedures to be updated, and to identify any new risks. Management will be responsible for ensuring this policy is complied with. Where considered appropriate, independent audits will also be conducted.

- **Compliance**. We specifically ensure compliance with the General Data Protection Regulations 2018, the Privacy and Electronic Communications Regulations, and the latest version of PCI DSS.
- **Incident Management**. Anyone who has access to The Place Information Systems is required to immediately report a suspected issue in relation to this policy (e.g. security breach) to their line manager, HR or the IT Help Desk.

**Data Collection and Processing**

We process and store data only for the purpose specified when data is collected (see above). Customer data is kept for us to keep users informed about our services; to monitor service users for reporting purposes (for which data will be anonymised); and to respond to enquiries and to market our services.

Participant medical information is collected only for the purpose of safe practice (see below) and is obtained with the written consent of the adult participant or the parent/guardian for participants aged under 12.

Participant, employee and business associate/partner financial information is kept for billing and accounting purposes, to allow us to make and receive payments.

We will never sell participant, employee, volunteer or trustee data to any third party. Please also see our Data Retention policy.

Data collected for our LCDS students is covered by the Student Privacy policy and includes details of what data is collected, how the data is used and who it is shared with. Please refer to this policy which can be found on our website for further details.

**Special Categories of Data**

Data about: health, ethnic origin, religious or political opinions, sexual life, criminal convictions is identified by the GDPR as “special categories of data”, and this information requires additional conditions to be met before it can be processed. We may collect and process such information in order to comply with legal obligations on equal opportunities monitoring, to comply with employment law, and for the purposes of running participatory activities safely.

When collecting and processing data in one or more of these special categories, we will outline the specific purpose of the data collection at the point of collection and seek explicit consent when collecting health information to be used to enable safe practice in the delivery of learning activities.

**Related Documents**

Documents to be read in conjunction with this Policy:

- Place Privacy policy as found on our website Complaints, Freedom of Information and Privacy Policy | The Place
- Student Privacy notice: Student Policies | The Place

- IT and Communications Acceptable Usage Policy
- Mobile Device and BYOD (Bring Your Own Device) Acceptable Usage policy
- Subject Access Request procedure
- Rectification and Erasure process
- Data Breach and Incident reporting policy and procedure
- Student Communications Policy and Guidelines

**Related Legislation: The Freedom of Information Act**

The Act pre-dates the GDPR legislation by some years, and gives the public a general right of access to information held by public authorities. Although not a public authority itself, The Place has responsibilities under the act under the regulation of the Office for Students (OfS) and the National Portfolio Organisation grant terms and conditions set out by Arts Council England (ACE). Should a Freedom of Information request to access information held by OfS or ACE concerning The Place be made, we are obliged to agree to that information being made public.

**Privacy, Data Protection and Information Security Policy Agreement**

I confirm that I have read and understood the Privacy, Data Protection and Information Security Policy (this document).

I understand that I am required to:

- Follow the principles of this policy
- Attend or undertake IT Data Protection & Security training or e-learning within one month of joining
- Identify, read and follow all additional relevant procedures to my role where they currently exist
- Report privacy or security issue to my Line Manager, Head of HR and the IT Help Desk immediately

I understand that contravention of this Policy or any of these procedures may be deemed to be a disciplinary offence.

| | |
|---|---|
| **Employee name** | |
| **Department** | |
| **Signed** | |
| **Date** | |

**This policy is not contractual and therefore may be subject to change. However, it does set out how we normally deal with such issues and therefore the content should be regarded as a reasonable management instruction.**

## Appendix 1: Lawful Basis for Processing Personal Data

The GDPR provides six lawful bases for processing personal data. The Place will only process personal data where it is necessary and it has identified at least one valid lawful basis, decisions on the appropriate lawful basis will be based on the specific purpose and context of the processing.

| | |
|---|---|
| **1. Public Task** | Data processing is necessary to perform a task in the public interest or for an official function. |
| **2. Contract** | Data processing is necessary for fulfilling a contract or to enter into a contract. |
| **3. Legal Obligation** | Data processing is necessary to comply with the law (excluding contracts). |
| **4. Vital Interest** | Data processing is necessary to protect the life of the individual, or another individual. |
| **5. Legitimate interest** | Data processing is necessary for the organisation's legitimate interests or the legitimate interest of another party, unless it would undermine the interests of an individuals' right to privacy. |
| **6. Consent** | Consent must be freely given, specific, informed and unambiguous. The data subject must be informed of their absolute right to withdraw consent at any time. |

Before processing of personal data begins, The Place staff are responsible for ensuring that:

- There is no other way to reasonably achieve the same outcome, without processing personal data,
- Valid lawful bases and justifications for processing personal data have been identified and documented. There may be more than one lawful basis, in which case they should all be identified and recorded,
- Information about the lawful basis and intended purpose for processing information is included in the privacy notice (for example: The Place has obtained the explicit consent of the individual; it is necessary to protect the vital interest of an individual/s; the information had already been made public by the individual; or it necessary for purposes in the public interest, academic research purposes or statistical purposes).
- In instances where sensitive personal (special category) data, criminal convictions data, or data about offences will be processed; The Place will have identified an additional condition for processing, as described in GDPR Article 9: Processing of special categories of personal data (see also Special Categories of Data in the policy above).

Other conditions for processing special category information exist and can be found in Article 9 of the GDPR. If any member of The Place is in any doubt about these matters, they should consult the Head of Operations.

## Appendix 2: Rights of Access to Data (Subject Access Requests)

Individuals have the right to obtain confirmation from The Place as to whether the organisation is processing personal data about them, and where that is the case, access to their personal data. Where The Place is processing a large quantity of data concerning a data subject, it will request that, before the information is delivered, the individual specifies the information or processing activities to which the request relates.

Any individual who wishes to exercise this right can request access either in writing or verbally. Requests can be made to any member of staff. Any such requests will be complied with within one calendar month of receipt of the request.

For further information, please see The Place Subject Access Request procedure.