



## **Data Protection Policy**

### **Introduction & Background**

Space2Create is committed to compliance with all national UK laws in respect of personal data, and to protecting the rights and privacy of individuals whose information the organisation collects in accordance with the General Data Protection Regulation and the UK Laws that implement it (**Data Protection Legislation**).

The purpose of the Data Protection Legislation is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge.

This Data Protection Policy is designed to ensure that Space2Create complies fully with Data Protection Legislation and that personal data is fairly, lawfully and transparently processed.

The Data Protection Legislation applies to all personal data throughout its lifespan, from the point of collection to its eventual destruction. Personal data includes any piece of information which enables the identification of a living individual, such as a name, contact details and health information.

If personal data exists in any form, whether electronic or in a paper-based filing system, it is covered by the Data Protection Legislation.

The policy applies to all trustees, staff, volunteers and service users of the organisation and third-party contractors and will be accessible to all.

### **Purpose and aims of this Policy**

To protect the rights and privacy of living individuals who access Space2Create services, work for, or support Space2Create. To ensure that personal data is not used, stored or disclosed ('processed') without such individual's knowledge, and is processed with a lawful basis and in a fair and transparent manner.

### **Policy Statement and Our Commitment to Legal Principles**

When processing personal data in the context of your involvement with Space2Create, you must comply with the six principles of good practice identified in Article 5 of the GDPR. These principles outline the following:

- **Lawfulness & Fairness:** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
- **Purpose Limitation:** Personal data shall be 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 purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

- **Data Minimisation:** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Accuracy:** Personal data shall be 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.
- **Storage Limitation:** Personal data shall be 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 be 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 the GDPR in order to safeguard the rights and freedoms of individuals; and
- **Security:** Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In simple terms, this means that Space2Create must collect and use personal data fairly, tell people how their personal data will be used, that it will be stored safely and securely and not disclose it unlawfully to third parties. Space2Create needs to be careful that the information collected is relevant and that the organisation does not collect more information than is needed for the stated purpose.

Partners and any third parties (including visiting artists) working with or for the organisation, will not have access to personal data and will be expected to comply with the principles of this Policy.

### **Individuals' Rights**

Individuals have the following rights regarding data processing, and the data that is recorded about them:

1. The right to be informed about how we process their personal data
2. The right to access their personal data
3. To right to rectify their personal data
4. To right to have their personal data erased
5. The right to restrict processing
6. The right to have a copy of their personal data in a portable form
7. The right to object to direct to marketing and profiling
8. Rights in relation to automated decision making and profiling.

### **Data Collection and Lawful Processing**

Data Minimisation is important to think about prior to the collection of any personal data and Space2Create will only collect information that is absolutely necessary.

Data owners must ensure that they have a lawful basis for processing personal data. Under the GDPR there are 6 lawful bases for processing non-sensitive personal data as follows; consent or as is necessary as part of a contract, to comply with a legal obligation, to protect the vital interests of an individual, to fulfil a public task or as part of the organisation's legitimate interests (provided the latter is balanced against the rights of the individual).

Stricter rules apply to sensitive personal data (or special categories of personal data), such as information about a person's health, ethnic origin or religious beliefs as well as information about criminal offences. Space2Create will only collect this information under very limited circumstances – for example, the person has given explicit consent or it is necessary for specific reasons permitted by law.

### **Consent and Transparency**

Personal data should not be obtained, held, used or disclosed unless the individual has given consent or there is another lawful basis that allows us to do so. The organisation understands “consent” to mean that the data subject has been fully informed of the intended processing and has signified (by an affirmative action) their freely given agreement preferably in writing, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

Space2Create will make information regarding available privacy notices on relevant data collection forms to clients explaining how we process their information. Space2Create must provide privacy notices even if we do not need to ask for consent.

### **Security of Data and Storage of Data**

All staff are responsible for ensuring that any personal data which the organisation holds and for which they are responsible, is kept securely and is not disclosed to any third party unless that third party has been specifically authorised by the organisation to receive that information and has entered into a confidentiality agreement.

Staff, volunteers and trustees must not remove personal data from Space2Create premises either in electronic or paper form unless it is really necessary – for example, in cases where staff have to attend external meetings, etc. In instances where data is taken out of Space2Create premises, such data must be fully encrypted and password protected. If data is in a paper format, the staff member handling such data should ensure that any names of people and/or any information that could lead to identification of subject individuals is transported and stored securely.

Personal data pertaining to service users should be stored securely in Space2Create and not be taken out of the office in paper or electronic format. Staff can access Office 365 remotely but will only access personal data away from S2C in an emergency situation.

### **Disclosure of Data**

Space2Create must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party.

### **Retention & Deletion of Data**

Personal data may not be retained for longer than it is required, e.g. after a member of staff / service user has left, personal data will be kept for 1 month before being securely deleted electronically and the paper copy shredded.

Personal data may need to be kept for a certain period of time under other legislation such as accounting or tax laws. In such cases reasonable measures must be taken to ensure it is kept securely in accordance with industry standards.

Office365 is where data collection forms will be stored electronically and a hard copy is stored in the locked filing cabinet.

### **Personal Data Breaches**

All staff, volunteers and visiting artists have a responsibility to report all breaches to the CEO who will decide how to respond to the breach and whether it needs to be notified.

### **Anonymisation**

Anonymisation is the process of removing information that could lead to an individual being identified (for example, names and other obvious identities which reveal the identity of the individual). Personal data should be anonymised whenever it is practical and appropriate to do so. Anonymising personal data significantly reduces the risks to individuals if that information is compromised.

Where personal data is collected and needs to be retained for statistical purposes, but it no longer needs to be attributable to an individual, Space2Create will anonymise this at the earliest opportunity.

### **Roles and Responsibilities**

#### **Senior Management**

Overall responsibility for compliance with Data Protection Legislation rests with the CEO who is responsible for making sure that the Data Protection function is fully resourced to meet the needs of the Charity.

#### **Trustees and the CEO**

The CEO is responsible for promoting data protection awareness and compliance with Data Protection Legislation and this Policy with staff. The Operations Manager has the responsibility for sharing this with volunteers and the Well-being Manager is responsible for sharing this with service users.

#### **All Staff, Volunteers and Trustees**

It is the responsibility of all trustees, staff and volunteers to ensure they understand and act in accordance with this Policy and Data Protection Legislation.

Staff, volunteers and trustees should also ensure that they keep the CEO updated if they become aware of any proposed changes or changes to the ways in which personal data is being processed by their team.

Staff, volunteers or trustees found to be acting contrary to this Policy may be subject to disciplinary action. This is because any breach of the Data Protection Legislation could result in Space2Create facing legal action.

#### **How does it affect me?**

Space2Create could be fined if anybody uses or discloses information about other people without their consent or reliance on other lawful grounds. In order to help keep personal data secure, staff, volunteers and trustees should take particular care when using the Internet, e-mail and the management information systems or talking on mobile or landline telephones. You will be committing an offence if you steal or recklessly misuse personal data.

Special care must be taken with sensitive personal data (or special categories of personal data) such as information relating to race, ethnic origins, religious/political beliefs, health data, disabilities, sexual life, genetics, biometrics or trade union membership. Details of criminal offences or alleged offences must also be handled with special care.

Any breach of the Data Protection Legislation or this Policy will be dealt with under Space2Create's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

### **Prepare for someone wanting to see their data**

A 'subject access request' is the formal term for what happens when anyone asks you for a copy of information you hold about them. They could ask verbally, in writing or even on social media. You have one month to gather the data you have and provide it to them in a secure way.

For S2C this should be a case of either, printing off and sending securely or emailing as an attachment, their data collection form saved in a folder in OneDrive.

Subject access requests for additional information or email communication may require careful consideration:

You'll need to:

- plan for requests to come in
- make sure you know how you'll find all the information
- make sure the information you hand over doesn't contain information about any other people
- know how to ask for time extensions if you need them
- have a plan to make sure you provide the information securely.

### **Steps to avoid a Data Breach**

#### **Space2Create will:**

- check and update systems regularly
- make sure all trustees, staff, volunteers and service users know not to share data
- make sure all trustees, staff, volunteers and service users know how to report a breach (however minor the risk)
- be clear that the organisation needs to know what has happened as quickly as possible so it can take actions and learn.

Get ready for things going wrong by having procedures or steps to follow.

- Decide when you need to let the people who could be affected know and how you will do this.
- Check whether the breach meets the rules that mean you must report it to the ICO within 72 hours of being made aware of it.
- Include the ICO small organisation helpline in your procedures to help you (0303 123 1113).
- Update your data processing procedures to reduce the risk of it happening again.
- Develop training to reduce future risks.