response. ability. theatre.

GDPR Data Protection Policy

1. **Policy, scope and objectives**

The Board of Trustees of Response Ability Theatre (hereafter referred to as RAT) is committed to complying with all relevant UK laws in respect of personal data, and to protecting the "rights and freedoms" of individuals whose information it processes in accordance with the UK General Data Protection Regulation, the Data Protection Act 2018 and all relevant legislation and regulations in force from time to time (collectively referred to as 'GDPR' in this document).

The scope of this document includes all the activities of RAT, including fundraising, workshops and trainings, research and participation projects, productions and events, lectures, and support to individuals, both on and offline and using various channels. This is not an exhaustive list and may be updated from time to time in the future.

RAT is committed to complying with GDPR and maintains the following policies and procedures to ensure good practice:

A. PRIVACY POLICY

This is our overarching policy statement which explains to data subjects how we process personal information, which includes supporters, beneficiaries, staff and volunteers. Our Privacy Policy is available on our website in order to clearly communicate our best practice approach to individuals' data processing.

B. CONSENT PROCEDURE

This procedure covers all situations where we require the consent of a data subject for the processing of personal data, such as to use their image in marketing or funding reporting material and/or their full names in case studies, to ensure that participants have understood /signed the consent form.

C. DATA PROCESSING & STORAGE PROCEDURES

There will be an **agreement between us and any external third-parties** where personal data is shared for the purpose of processing it. Depending on the destination of the shared data, an international data transfer agreement may be required for extra-jurisdictional data sharing.
We maintain a **log of all assets** we hold, along with details of the asset owner, storage location, type of data processed, retention period, security measures and who has access to that data.
Our **retention policy** ensures that all personal data is retained and destroyed in line with the requirements of GDPR.
Our **data breach notification procedure** is to report to the Information Commissioner's Office (hereafter referred to as the ICO) within 72 hours in the event of a data breach that could potentially lead to the accidental or deliberate destruction, loss, alteration, corruption or unauthorised disclosure of, or access to personal data, and to inform the data subject as soon as possible if the potential breach is high risk.
Our **subject access request procedure** recognises our responsibility to comply with a request from an individual, in accordance with their entitlement to ask us to disclose what personal data we hold / process on them. If requested, we are required to provide to them with their personal data, the purposes for which it is being processed and details of who has access to it, within a month of the request being made - unless the information requested is extensive, in which case we can request an extension.

This policy applies to all staff, volunteers and other interested parties of RAT such as outsourced suppliers. Any breach of GDPR will be dealt with by reference to our contracts with staff, or may lead to the termination of the engagement of a third-party supplier, and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Partners and any third-parties working with or for RAT, and who have or may have access to personal information, will be expected to have read, understood and to comply with our Privacy Policy. No processor or Sub Contractor may access personal data held by RAT without having first entered into a thid-party data confidentiality and protection agreement with us. This imposes on the third-party obligations no less onerous than those to which RAT is committed, and which gives RAT the right to audit Processors and third-parties in compliance with the agreement.

2. Responsibilities under the GDPR

RAT is a data controller under GDPR. All those in managerial or supervisory roles throughout RAT are responsible for developing and encouraging good information handling practices within the organisation.
The CEO is responsible for day-to-day GDPR procedures and policies and is the first point of contact for staff and volunteers seeking clarification on data protection compliance.

RAT is accountable to the Board of Trustees for the management of personal information within RAT and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

- Development and implementation of systems to protect personal data as required by this policy;
- Security and risk management in relation to compliance with the policy.

Compliance with data protection legislation is the responsibility of all members of RAT who process personal information.

Supporters, donors and other interested parties are responsible for ensuring that any personal data supplied by them, and that is about them, to RAT is accurate and up-to-date wherever possible.

3. Training

All staff and volunteers who access personal data are to be trained in GDPR as soon as is practical.
Training is an on-going requirement so the CEO will ensure that staff and any training materials / requirements are kept up to date and advise of any changes in the GDPR legislation.
RAT ensures that those with day-to-day responsibility for personal data are able to demonstrate compliance with GDPR and good practice.
All staff and volunteers must understand their responsibility to ensure that personal information is protected and processed in accordance with RAT's procedures, taking into account any related security requirements.

4. Risk Assessment

RAT assesses the level of risk to individuals associated with the processing of their personal information. Assessments will also be carried out in relation to processing undertaken by other organisations on behalf of RAT. RAT shall manage any risks which are identified by the risk assessment in the asset log in order to reduce the likelihood of a non-conformance with this policy.

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the "rights and freedoms" of natural persons, RAT shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

Where it is clear that RAT is about to commence processing of personal information that could have an adverse impact on the rights of data subjects, the decision as to whether or not RAT may proceed must be reviewed by the CEO. The CEO shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the ICO.

Appropriate controls will be selected to reduce the level of risk associated with processing individual data to an acceptable level, by reference to the requirements of GDPR.

5. Data protection principles

All processing of personal data must be done in accordance with the following data protection principles.

A. **Personal data must be processed lawfully, fairly and transparently**

RAT's Privacy Policy ensures transparency and easily accessible policies relating to the processing of personal data and the exercise of individuals' "rights and freedoms". Information is communicated to the data subject in an intelligible form using clear and plain language.

B. **Personal data must be adequate, relevant and limited to what is necessary for processing**

RAT is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is to be obtained, is not collected.

If data is given or obtained that is excessive or not specifically required by RAT's documented procedures, we are responsible for ensuring that it is securely deleted or destroyed in line with this policy.

C. **Personal data must be accurate and kept up to date**

Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

RAT is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

Staff, supporters, donors and volunteers should notify RAT of any changes in circumstance to enable personal records to be updated accordingly. RAT will make every effort to ensure records are accurate, but cannot be held responsible for inaccurate data if the data subject has not made reasonable effort to inform the organisation. It is the responsibility of RAT to ensure that any notification regarding change of circumstances is noted and acted upon.

RAT will regularly review all the personal data maintained, and will identify any data that is no longer required in the context of the registered purpose and will arrange to have that data securely deleted / destroyed. Records will be kept to ensure this process is demonstrable.

RAT reserves the right, however, to keep data that it may require to defend a legal claim or which it is otherwise legally obliged to retain.

RAT is responsible for making appropriate arrangements, where third-party organisations may have been passed inaccurate or out-of-date personal information, for informing them that the information is inaccurate and/or out-of-date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal information to the Processor or Sub-Contractor where this is required.

D. **Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing**

Where personal data is retained beyond the processing date, it will be anonymised or otherwise encrypted in order to protect the identity of the data subject in the event of a data breach.

Personal data will be retained in line with the retention policy and will be reviewed every two years. RAT accepts that 'Consent' from data subjects to receive marketing and fundraising messages is not permanent and will be reviewed. RAT is committed to upholding the rights and freedoms of data subjects and makes every effort possible to be clear and transparent about the reasons for processing data.

RAT must specifically approve any data retention that exceeds the retention periods, and must ensure that the justification is clearly identified and in line with the requirements of GDPR.

RAT accepts that there may be other times where the personal data that it holds on supporters and its customers may be deleted. They are acknowledged as:

- The data is no longer necessary for the purpose for which it was collected.
- The data subject has withdrawn Consent.
- The data subject's rights override the Legitimate Interests of RAT.
- The data subject has objected to marketing or other communications and RAT has decided to stop such messages even if its Legitimate Interests were proven to be valid and had not infringed the rights and freedoms of the subject or subjects in question.
- Where unlawful processing had been identified.
- Where there was a legal obligation on RAT but this has now ceased.

This is not an exhaustive list and will be regularly reviewed by RAT.

E. **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. Security controls will be subject to review on a regular basis.

F. **Personal data shall not be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.**

G. **The transfer of personal data outside of the EU is prohibited unless an appropriate risk assessment has been carried out to determine that there is adequate protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data. In assessing this, regard must be had to the following factors, and an appropriate international data transfer agreement must be in place:**

- the nature, sensitivity and volume of the information being transferred and whether data subjects are children or otherwise vulnerable or at risk;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;

- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and
- the security measures that are to be taken as regards the data in the overseas location.

6. Data subjects' rights

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

A. To make subject access requests regarding the nature of information held and to whom it has been disclosed.

B. To prevent processing likely to cause damage or distress.

C. To prevent processing for purposes of direct marketing.

D. To be informed about the mechanics of automated decision-taking process that will significantly affect them.

E. Not to have significant decisions that will affect them taken solely by automated process or to object to any automated profiling without consent.

F. To sue for compensation if they suffer damage by any contravention of GDPR.

G. To not have their data processed at all ("the right to be forgotten") subject to any overarching obligation for it to be retained, or to limit its processing or have inaccurate data corrected, destroyed or deleted.

H. To request the ICO to assess whether any provision of GDPR has been contravened.

I. The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

Data Subjects who wish to complain to RAT may do so to the contact details provided in the Privacy Policy published on RAT's website, or directly to the ICO.

7. The Legal Bases that RAT will use to process data

Data controllers must have a legal basis for processing personal data. RAT processes data under one or more of the following legal bases:

A. **Consent**

Consent must be informed and freely given (i.e. not under duress or induced by misleading information), and by way of a positive act that clearly affirms that a data subject agrees to the processing of their data for a particular purpose. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

Consent may be withdrawn at any time. Consent is not the only or the default legal basis relied upon, although a withdrawal of consent may invalidate another legal basis, such as legitimate interest.

In most instances consent to process personal and sensitive data is obtained routinely by RAT using standard consent documentation.

Where RAT provides services to children, parental, or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the EU Member State has made provision for a lower age limit – which may be no lower than 13).

IMPORTANT NOTICE: even if consent is not required to process someone's data in other ways, it is always required to send them e-mails or texts containing marketing, fundraising or promotional content (Privacy & Electronic Communications Regulations 2003).

B. **Legitimate Interest**

RAT has a legitimate interest in processing data in pursuance of its charitable objects, specifically:

- the advancement of arts in particular but not exclusively theatre and the performing arts by involving people whose lives have been significantly affected, or who are at risk of being significantly affected by trauma;
- the advancement of education on the nature of trauma and trauma-conscious working practices, especially those in positions of care, on the causes, symptoms and management of trauma (awareness) through the use of the arts, in particular but not exclusively theatre and the performing arts, and to communicate learnings from research projects that directly or incidentally further understanding of trauma in theatre and arts-based ways for public consumption (learning); and
- the preservation and protection of physical and mental health by using the arts as a form of protection against and management of trauma.

These activities will routinely require the processing of personal data, and to facilitate these objectives we also engage in activities to raise funds and inform supporters about our work, including through events, campaigns and promotional communications. This in turn involves working with staff, volunteers and other stakeholders whose data we process.

These legitimate interests are subordinate to the rights of data subjects who may exercise those rights by asking us not to process their data in certain ways or at all. If they do so, we must comply, unless another overriding legal basis for processing data applies, such as a legal obligation.

If it can be demonstrated that our Legitimate Interest does not override the rights and freedoms of those data subjects with which it may have in the past, we may resume and further pursue our Legitimate Interest in the future. This will only ever be done after careful consideration of the GDPR, Prior Consultation Article 36.

We reserve the right to pursue and keep under review our Legitimate Interest with any data subject, who may in the future either, make a donation, leave us a legacy or major gift, purchase a ticket from us, engage in an educational project or be involved in a research programme, that we believe may be able to help us fulfil our aims and objectives as an organisation. We will do this using all lawful conditions available to us and within GDPR.

RAT will document all aspects relating to our Legitimate Interest and it will be continuously assessed to ensure that it remains valid and legitimate.

C. **Necessary for Contract**

Personal data may be processed where it is necessary in relation to a contract or agreement which a data subject has entered into or because they have asked for something to be done so they can enter into a contract or agreement. This might be a contract of employment or a ticket purchased from us for an event, for example.

In such cases, our processing of their data relates only to the contract that has or may be entered into, including where necessary, once the contract has included where there is a reason still to retain the data. We will not market or promote unrelated events or activities and will not fundraise to that data subject, promote events or educational projects to that data subject unless we have a Legitimate Interest to do so.

D. Legal Obligation

RAT will also process data where it has a legal obligation to do so, such as compliance with the requirements of public or regulatory bodies such as HMRC, the Charity Commission or for the purposes of safeguarding at-risk individuals or the prevention of crime. A legal obligation may require the retention of some, even if not all of a data subject's information, notwithstanding the assertion by them of their other data protection rights under.

8. Security of data

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

All personal data should be accessible only to those who need to use it. RAT has carefully considered the sensitivity and value of the information in question. Therefore, it has been decided that personal data will be kept:

- If paper based, in a lockable room with controlled access.
- If computerised, password protected. Care must be taken to ensure that PC screens and terminals are not visible except to authorised staff of RAT.

Paper records may not be left where they can be accessed by unauthorised personnel. Personal data may only be deleted or disposed of in line with the Data Retention Policy. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and destroyed before disposal.

9. Rights of access to data

Data Subjects have the right to access any personal data (i.e. data about them) which is held by RAT in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by RAT, and information obtained from third-party organisations about that person.

10. Disclosure of data

RAT 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. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of RAT's business.

GDPR permits certain disclosures without consent so long as the information is requested or necessary to be shared for one or more of the following purposes:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- safeguarding of children or adults at risk, or to prevent serious harm to a third-party;
- to protect the vital interests of the individual, this refers to life and death situations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork.

11. Retention and disposal of data

Personal data may not be retained for longer than it is required. RAT fully understands its obligations under GDPR to securely delete data no longer required for the purpose it was collected, or where a data subject has requested to be forgotten. However, it reserves the right under the GDPR to retain the data in an encrypted form should it require the data for a legal purpose or reason or for research purposes. RAT fully understands that to contact the data subject for any reason other than these would be a breach of data protection and an infringement of that data subject's rights and freedoms.

Personal data must be disposed of in a way that protects the “rights and freedoms” of data subjects, e.g. shredding, disposal as confidential waste, or secure electronic deletion.

Last updated: 03/07/2024