REVEAL THEATRE COMPANY

Controlled Document

Document Name:	**Data Protection Policy**
Document Reference Number:	**POL1**
Document Version Number	1
Date of approval by directors:	X
Review Schedule	Every two years
Next review due	X
Owner (Responsibility)	Julia Barton, Director
Revision History	See appendix

Document Description

This document outlines our legal requirements under the General Data Protection Regulations and the processes for how Reveal Theatre Company meets them. Note: GDPR came into force on 28 May 2018.

Implementation and Quality Assurance

Implementation is immediate and this Policy shall stay in force until any alterations are formally agreed.

The Policy will be reviewed every two years by the directors, sooner if legislation, best practice or other circumstances indicate this is necessary.

All aspects of this Policy shall be open to review at any time. If you have any comments or suggestions on the content of this policy, please contact Julia Barton at julia.barton@revealtheatre.co.uk

Data Protection Policy

Introduction

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give citizens back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR takes effect it will replace the data protection directive (officially Directive 95/46/EC) from 1995. The regulation was adopted on 27 April 2016 and applies from 25 May 2018 after a two-year transition period..

The 1998 Data Protection Act, which came into force on 1 March 2000, will continue to apply until the new General Data Protection Regulations come into force in May 2018.

The following guidance is not a definitive statement on the Regulations, but seeks to interpret relevant points where they affect Reveal Theatre Company ('RTC').

The Regulations cover both written and computerised information and the individual's right to see such records.

It is important to note that the Regulations also cover records relating to staff and volunteers.

All RTC staff are required to follow this Data Protection Policy at all times.

The directors of RTC have overall responsibility for data protection within RTC but each individual processing data is acting on the controller's behalf and therefore has a legal obligation to adhere to the Regulations.

RTC does not in its ordinary course of business hold data upon its clients, save for the purposes of statutory requirement or as required under Home Office/ PREVENT contracts. In the normal course of its business, RTC does prepare practitioner's reports that are provided to contract commissioners with the information about the efficacy of delivery, however these are generally anonymised and are destroyed as soon as they have been utilised. The most common data retained by RTC relates to personal data in respect of employees/practitioners.

Definitions

Processing of information – how information is held and managed.
Information Commissioner - formerly known as the Data Protection Commissioner.
Notification – formerly known as Registration.
Data Subject – used to denote an individual about whom data is held.
Data Controller – used to denote the entity with overall responsibility for data collection and management. RTC is the Data Controller for the purposes of the Act.
Data Processor – an individual handling or processing data
Personal data – any information which enables a person to be identified
Special categories of personal data – information under the regulations which requires the individual's explicit consent for it to be held by the Charity.

Data Protection Principles

As data controller, RTC is required to comply with the principles of good information handling.

These principles require the Data Controller to:

1. Process personal data **fairly**, **lawfully and in a transparent manner.**
2. Obtain personal data only for one or more **specified** and **lawful purposes** and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained.
3. Ensure that personal data is **adequate**, **relevant and not excessive** for the purpose or purposes for which it is held.
4. Ensure that personal data is **accurate** and, where necessary, **kept up-to-date.**
5. Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
6. Ensure that personal data is kept secure.
7. Ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates.

Consent

RTC must record service users' explicit consent to storing certain information (known as 'personal data' or 'special categories of personal data') on file.

For the purposes of the Regulations, personal and special categories of personal data covers information relating to:

1. The racial or ethnic origin of the Data Subject.
2. His/her political opinions.
3. His/her religious beliefs or other beliefs of a similar nature.
4. Whether he/she is a member of a trade union.
5. His/her physical or mental health or condition.
6. His/her sexual life.
7. The commission or alleged commission by him/her of any offence
8. Online identifiers such as an IP address
9. Name and contact details
10. Genetic and/or biometric data which can be used to identify an individual

Whilst RTC do not in the normal course of business hold personal data other than information held about freelance workers, such information will, in the main, relate to bank details and contact information in that respect.

Consent is not required to store information that is not classed as special category of personal data as long as only accurate data that is necessary for a service to be provided is recorded.

As a general rule RTC will always seek consent where personal or special categories of personal information is to be held.

It should also be noted that where it is not reasonable to obtain consent at the time data is first recorded and the case remains open, retrospective consent should be sought at the earliest appropriate opportunity.

If personal and/or special categories of personal data need to be recorded for the purpose of service provision and the service user refuses consent, the case should be referred to the Julia Barton for advice.

Obtaining Consent

Consent may be obtained in a number of ways depending on the nature of the interview, and consent must be recorded on or maintained with the case records:

- face-to-face
- written
- telephone
- email.

Face-to-face/written

A pro-forma should be used.

Telephone
Verbal consent should be sought and noted on the case record.

E-mail
The initial response should seek consent.

Consent obtained for one purpose cannot automatically be applied to all uses e.g. where consent has been obtained from a service user in relation to information needed for the provision of that service, separate consent would be required if, for example, direct marketing of insurance products were to be undertaken.

Preliminary verbal consent should be sought at point of initial contact as personal and/or special categories of personal data will need to be recorded either in an email or on a computerised record. The verbal consent is to be recorded in the appropriate fields on the computer record or stated in the email for future reference. Although written consent is the optimum, verbal consent is the minimum requirement.

Specific consent for use of any photographs and/or videos taken should be obtained in writing. Such media could be used for, but not limited to, publicity material, press releases, social media, and website. Consent should also indicate whether agreement has been given to their name being published in any associated publicity. If the subject is less than 18 years of age, then parental/guardian consent should be sought.

Individuals have a right to withdraw consent at any time. If this affects the provision of a service(s) by RTC then the practitioner should discuss with Julia Barton at the earliest opportunity.

Ensuring the Security of Personal Information

Unlawful disclosure of personal information

1. It is an offence to disclose personal information ‘knowingly and recklessly’ to third parties.

2. It is a condition of receiving a service that all service users for whom we hold personal details sign a consent form allowing us to hold such information.

3. Service users may also consent for us to share personal or special categories of personal information with other helping agencies on a need to know basis.

4. A client’s individual consent to share information should always be checked before disclosing personal information to another agency.

5. Where such consent does not exist information may only be disclosed if it is in connection with criminal proceedings or in order to prevent substantial risk to the individual concerned. In either case permission of Julia Barton should first be sought.

6. Personal information should only be communicated within RTC's staff and freelance practitioners on a strict need to know basis. Care should be taken that conversations containing personal or special categories of personal information may not be overheard by people who should not have access to such information.

Ethnic Monitoring

In order for RTC to monitor how well our staff and practitioners reflect the diversity of the local community we may in the future request that they complete an Equality and Diversity Monitoring form. The completion of such form would be voluntary, although strongly encouraged. Responses would be securely stored and held on a passworded database for statistical purposes only.

Use of Files, Books and Paper Records

In order to prevent unauthorised access or accidental loss or damage to personal information, it is important that care is taken to protect personal data. Paper records should be kept in locked cabinets/drawers overnight and care should be taken that personal and special categories of personal information is not left unattended and in clear view during the working the day. If your work involves you having personal and/or special categories of personal data at home or in your car, the same care needs to be taken.

Disposal of Scrap Paper, Printing or Photocopying Overruns

Be aware that names/addresses/phone numbers and other information written on scrap paper are also considered to be confidential. Please do not keep or use any scrap paper that contains personal information but ensure that it is shredded.

If you are transferring papers from your home or your venue for work this should be done as soon as possible and not left in a car. When transporting documents they should be carried out of sight in the boot of your car.

Computers

Where computers are networked, access to personal and special categories of personal information is restricted by password to authorised personnel only.

Computer utilised by staff and freelance practitioners operating on behalf of RTC should be positioned in such a way so that passers-by cannot see what is being displayed if and when any confidential information is to be displayed. If this is not possible then privacy screens should be used on the monitor to afford this level of protection. If working in a public area, eg at a school, you should lock your computer when leaving it unattended.

Firewalls and virus protection to be employed at all times to reduce the possibility of hackers accessing our system and thereby obtaining access to confidential records.

Where computers or other mobile devices are taken for use off the premises the device must be password protected.

Cloud Computing

At present RTC do not operate a cloud based system for storage. However, and in the future when commissioning any cloud based systems, RTC will satisfy themselves as to the compliance of data protection principles and robustness of the cloud based providers.

Privacy Statements

Any documentation which gathers personal and/or special categories of personal data should contain the following Privacy Statement information:

- Explain who we are
- What we will do with their data
- Who we will share it with
- Consent for marketing notice
- How long we will keep it for
- That their data will be treated securely
- How to opt out
- Where they can find a copy of the full notice

A fuller Privacy Statement will also be published on our website.

Personnel Records

The Regulations apply equally to freelance practitioners and staff records. RTC may at times record special categories of personal data with the volunteer's consent or as part of a staff member's contract of employment.

For staff and practitioners who are regularly involved with children in schools, it will be necessary for RTC to apply to the Disclosure & Barring Service to request a disclosure of

spent and unspent convictions, as well as cautions, reprimands and final warnings held on the police national computer. Any information obtained will be dealt with under the strict terms of the DBS Code. Access to the disclosure reports is limited to the directors of RTC. If there is a positive disclosure the directors of RTC will consider that disclosure and our insurers to assess the risk of appointment. Insurers should not see the report itself.

Confidentiality

When working from home, or from some other off-site location, all data protection and confidentiality principles still apply. All computer data, e.g. documents and programmes related to work for RTC should not be stored on any external hard disk or on a personal computer unless prior authorisation and risk assessments have been completed and should be appropriately password protected and encrypted.

Workstations in areas accessible to the public, e.g. a school, should operate a clear workstation practice so that any paperwork, including paper diaries, containing personal and/or special categories of personal data is not left out where passers-by could see it.

When sending emails to outside organisations, e.g. schools, universities or PREVENT, care should be taken to ensure that any identifying data is removed and that codes (e.g. initials or identifying code number etc.) are to be used wherever possible. Confidential and/or special categories of personal information should be written in a separate document which should be password protected before sending. Wherever possible, this document should be 'watermarked' confidential.

Any paperwork kept away from the office (eg reports upon practice delivery) should be treated as confidential and kept securely as if it were held in the office. Documents should not be kept in open view (eg on a desktop) but kept in a file in a drawer or filing cabinet as examples, the optimum being a locked cabinet but safely out of sight is a minimum requirement.

If you are carrying documents relating to a number of clients when on a series of school visits, you should keep the documents for other clients locked out of sight in the boot of the car (not on the front seat) and not take them into the clients premises. When carrying paper files or documents they should be in a locked briefcase or in a folder or bag which can be securely closed or zipped up. The briefcase/folder/bag should contain RTC's contact details. Never take more personal data with you than is necessary for the job in hand. Care should be taken to ensure that you leave a client's home with the correct number of documents and that you haven't inadvertently left something behind.

Retention of Records

Paper records should be retained for the following periods at the end of which they should be shredded:

- Client records – 6 years after ceasing to be a client.
- Staff records – 6 years after ceasing to be a member of staff.
- Unsuccessful staff application forms – 6 months after vacancy closing date.
- Volunteer records – 6 years after ceasing to be a volunteer.
- Timesheets and other financial documents – 7 years.
- Employer's liability insurance – 40 years.
- Other documentation, eg practitioner's reports, should be destroyed as soon as it is no longer needed for the task in hand.

Archived records should clearly display the destruction date.

What to Do If There Is a Breach

If you discover, or suspect, a data protection breach you should report this to Julia Barton who will review our systems, in conjunction with the other director(s) to prevent a reoccurrence. Upon any suspected breach the directors shall determine any action to be taken, together with analysis of any outcomes to determine whether it needs to be reported to the Information Commissioner. There is a time limit for reporting breaches to ICO and therefore any suspected breaches must be reported to Julia Barton immediately it becomes apparent.

Any deliberate or reckless breach of this Data Protection Policy by an employee or practitioner may result in disciplinary action which may result in dismissal or termination of contract.

The Rights of an Individual

Under the Regulations an individual has the following rights with regard to those who are processing his/her data:

- Personal and special categories of personal data cannot be held without the individual's consent (however, the consequences of not holding it can be explained and a service withheld).

- Data cannot be used for the purposes of direct marketing of any goods or services if the Data Subject has declined their consent to do so.

- Individuals have a right to have their data erased and to prevent processing in specific circumstances:
    - Where data is no longer necessary in relation to the purpose for which it was originally collected
    - When an individual withdraws consent
    - When an individual objects to the processing and there is no overriding legitimate interest for continuing the processing
    - Personal data was unlawfully processed
- An individual has a right to restrict processing – where processing is restricted, RTC is permitted to store the personal data but not further process it. RTC can retain just enough information about the individual to ensure that the restriction is respected in the future.
- An individual has a 'right to be forgotten'.

RTC will not undertake direct telephone marketing activities under any circumstances.

Data Subjects can ask, in writing to Julia Barton, to see all personal data held on them, including e-mails and computer or paper files and such requests must be complied with within 30 days of receipt of the written request.

Cookies

Cookies are small encrypted text files that may be stored on your computer or other device by Reveal Theatre website. Our website may use cookies to collect information about the way you access the site, but cannot identify you personally.

We may use cookies for the following reasons:

- To provide site usage information (Google Analytics), which will help us continue to improve and develop the products and services we offer. These cookies collect information about how visitors use a website, for instance which pages visitors go to most often, and if they get error messages from web pages. These cookies don't collect information that identifies a visitor. All information these cookies collect is aggregated and therefore anonymous. It is only used to improve how a website works.
- By using our website, you agree that we can place these types of cookies on your device.
- To analyse your use of our website, allowing us to identify customer preferences and improve customers' experience of the website.

You can adjust your web browser preferences to disable cookies. To find out how to reject or restrict cookies you may find it helpful to visit https://ico.org.uk/for-the-public/online/cookies/. Please note that some cookies may be essential to make

purchases or request information on this website. Should you decide to reject cookies, the ability of the website to provide the service you request may be impaired.

Powers of the Information Commissioner

The following are criminal offences, which could give rise to a fine and/or prison sentence

- The unlawful obtaining of personal data.
- The unlawful selling of personal data.
- The unlawful disclosure of personal data to unauthorised persons.

Further Information

Further information is available at www.informationcommissioner.gov.uk

Details of the Information Commissioner

The Information Commissioner's office is at:

Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Switchboard*:* 01625 545 700
Email: mail@ico.gsi.gov.uk
Data Protection Help Line: 01625 545 745
Notification Line: 01625 545 740

Revision History

Revision date	Summary of Changes	Other Comments