KINGSTON THEATRE TRUST

DATA PROTECTION, PRIVACY POLICY & CODE OF PRACTICE – PERSONNEL

1. Introduction

In accordance with the General Data Protection Regulation (GDPR) of May 25th 2018, the data controller is Kingston Theatre Trust (KTT) trading as Rose Theatre Kingston (also referred to here as the Rose).

The term **personnel** when used in this Policy shall include any person or individual who is, or has been, an employee of the Rose and/or who will be placed onto the Rose's payroll and shall also include contract workers and/or agency staff employed at the Rose's premises, or working directly on the Rose's behalf, as well as volunteers, interns, apprentices and committee members.

The Rose is committed to being transparent about how it collects and uses the personal data of its personnel, and to meeting its data protection obligations. This policy sets out the Rose's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of job applicants, employees, freelancers, casual workers, contractors, volunteers, interns, apprentices, committee members and former employees, referred to here as personnel or HR-related personal data.

This policy does not apply to the personal data of clients, trustees or other personal data processed for business purposes. The general Privacy & Cookie Policy is available at the following link: https://www.rosetheatrekingston.org/privacy-cookies-policy

2. Data Protection Team (here referred to as DPT)

Your contact for any HR related queries is: Lesley Rowden (Theatre Manager) – email lesleyr@rosetheatrekingston.org
Your contact for any customers' related queries is: Paola Pozzi (Head of Marketing & PR) – email paolap@rosetheatrekingston.org
Your contact for any development related queries is: Kristen Gallagher (Development Director) – email kristeng@rosetheatrekingston.org

Overall responsibility and authority for all privacy and data protection matters lies with: Robert O'Dowd (Chief Executive) – email roberto@rosetheatrekingston.org

Other staff members (such as Head of Depts) may also be handling employee personal data, they are therefore responsible for determining the purposes and the manner in which any personal data are to be processed to ensure it complies with this Policy.

The Data Protection Team has overall responsibility for the implementation of this policy. If employees have any questions about data protection in general, this policy or their obligations under it, they should direct them to the DPT.

3. Data protection principles

Personal data is any information that relates to a living individual who can be identified from that information. **Processing** is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

Under the GDPR, the Rose processes HR-related personal data in accordance with the following data protection principles:

- The organisation processes personal data lawfully, fairly and in a transparent manner.
- The organisation collects personal data only for specified, explicit and legitimate purposes.
- The organisation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The organisation keeps personal data only for the period necessary for processing.
- The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

4. Personal data relating to personnel

The Rose holds information in its personnel files relating to past, present and potential future employees. It collects and processes such data in order to meet its legitimate interests as an employer to comply with statutory requirements and to fulfil individual employment contracts with its employees.

A personnel record is any printed or handwritten document, digitised image, sound recording or computer file which:

- refers by name - or any other means of identification - to a current, potential or past employee. Information includes, but is not limited to, name, address, date of birth, gender, employment history, bank account, national insurance number; and
- represents any information about any matter relating to an employee (whether past, present or future) of a potentially private or sensitive nature.

The Rose collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the Rose collects personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal records checks permitted by law. The Rose will seek information from such third parties with your consent only.

5. Purposes for holding data on personnel files

The Rose needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.

In some cases, the Rose needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. For certain positions, it is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

In other cases, the Rose has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the organisation to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- provide references on request for current or former employees;
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace.

The Rose will ensure that all personal information about an employee, including information in personnel files, is securely retained. Hard copies of information will be kept in a locked filing cabinet. Information stored electronically will be subject to access controls and passwords and encryption software will be used where necessary.

Where laptops are taken off site, employees must follow the Rose's relevant procedures relating to the security of information and the use of computers for working at home/bringing your own device to work (see section 10).

Where the Rose relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

6. Special categories of personal data

The GDPR refers to sensitive personal data as 'special categories of personal data' (see Article 9), these include:

- racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- physical or mental health or condition;
- sex life;
- commission or alleged commission of any criminal offence; and
- proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

The Rose will process any sensitive data, including sickness and injury records and references, in accordance with the data protection principles (see section 3) and in line with its legitimate interests to provide a safe environment for its employees. The Rose will retain sensitive personal data with the express consent of the employee in question.

The Rose may also collect relevant sensitive personal information from personnel for equal opportunities monitoring purposes. Data that the Rose uses for these purposes is anonymised or is collected with the express consent of the individuals in question, which can be withdrawn at any time. Personnel are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

7. Who access personnel files or HR-related data

Your information will be shared internally, including with members of the HR and recruitment team (including payroll), your line manager, managers in the business area in which you work and IT contractors if access to the data is necessary for performance of their roles.

The Rose may share your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service.

The Rose may share your data with third parties that process data on its behalf, for example in connection with payroll, the provision of benefits and the provision of occupational health services – third party organisations include Edenred Childcare Vouchers, Sage Payroll, Now Pension, SuperSaas and government bodies such as HMRC.

If the Rose were to enter into discussions about a merger or acquisition with a third party, it will seek to protect personnel data in accordance with the data protection principles.

8. Individuals' responsibilities regarding personal information (both their own and of other's)

Personnel are responsible for helping the Rose keep their personal data up to date. They should let the DPT know if data provided changes, for example if they move house or change their bank details.

Personnel who have access to the personal data of other individuals (and in some cases of our customers and clients) in the course of their employment, contract, volunteer period, internship or apprenticeship are also required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the Rose's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to the DPT immediately.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the Rose's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

9. Data security

The Rose takes the security of personal data seriously, and has a number of internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

In particular, personnel with authorized access to data need to ensure that:

- Papers are stored in lockable cabinets in secure offices when not being actively used;
- Electronic data is saved securely with access limited to only the members of the team who require it for the performance of their roles;
- Offices are secure and only personnel holding appropriate security passes can access them;
- Emails and or attachments are sent via a secured email network;
- When necessary data is disposed of or deleted securely.

Where information is disposed of, personnel should ensure that it is destroyed. This may involve the permanent removal of the information from the server, so that it does not remain in an employee's inbox or trash folder. Hard copies of information may need to be confidentially shredded. Personnel should be careful to ensure that information is not disposed of in a wastepaper basket/recycle bin.

If an individual acquires any personal information in error by whatever means, he/she shall inform the DPT immediately and, if it is not necessary for him/her to retain that information, arrange for it to be handled by the appropriate individual within the organisation.

Where an individual is required to disclose personal data to any other country, he/she must ensure first that there are adequate safeguards for the protection of data in the host country. For further guidance on the transfer of personal data outside the UK, please contact the DPT.

If an individual is in any doubt about what he/she may or may not do with personal information, he/she should seek advice from the DPT. If he/she cannot get in touch with the DPT, he/she should not disclose the information concerned.

Where the Rose engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

10. Taking personal data records off site

Personnel must not take personal data records off site (whether in electronic or paper format) without prior authorisation from the DPT.

Any individual taking records off site must ensure that he/she does not leave his/her laptop, other device or any hard copies of employment records on the train, in the car or any other public place. He/she must also take care when observing the information in hard copy or on-screen that such information is not viewed by anyone who is not legitimately privy to that information.

11. Retention

The Rose will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment will be no longer than is necessary for the purposes for which it is processed.

Application forms, interview records and references for unsuccessful internal and external candidates may be kept for a period of twelve months following the interview. If retention beyond this period is required, the Rose will obtain explicit consent from the individual. This applies to all manual files including any notes taken by anyone at interviews as well as computerised files.

All personnel data other than the name, job title, department and period of employment at the Rose will be deleted six years after employment has ended. Data relating to disciplinary and grievance records of current employees will be removed from personal files once they become spent in accordance with the Rose's disciplinary procedure and deleted three years from the date issued. Where disciplinary or grievance cases have involved concerns of sufficient severity or gravity data may be retained for longer periods.

12. Monitoring

The Rose may monitor personnel by various means including, but not limited to, recording their activities on CCTV, checking emails, listening to voicemails and monitoring telephone conversations. If this is the case, the Rose will inform individuals that monitoring is taking place, how data is being collected, how the data will be securely processed and the purpose for which the data will be used. The personnel will usually be entitled to be given any data that has been collected about him/her. The Rose will not retain such data for any longer than is absolutely necessary.

In exceptional circumstances, the Rose may use monitoring covertly. This may be appropriate where there is, or could potentially be, damage caused to the Rose by the activity being monitored and where the information cannot be obtained effectively by any non-intrusive means (for example, where an individual is suspected of stealing property belonging to the organisation). Covert monitoring will take place only with the approval of the Chief Executive.

13. Consequences of data breach and non-compliance

A personal data breach is: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service". A personal data breach can occur if there is unauthorised access within the organisation, or if a member of staff with lawful personal data access accidentally alters or deletes personal data.

As soon as you are made aware of a personal data breach, you must inform the DPT within 24 hours. Please include the following information:

- your name and contact details
- the date and time of the breach (or an estimate)
- the date and time you detected it
- basic information about the type of breach
- basic information about the personal data concerned

The Rose will record all data breaches regardless of their effect. If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will be its duty to inform the Information Commissioner (ICO) within 72 hours of discovery. We will also tell the affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures we have taken.

All personnel are under an obligation to ensure that they have regard to the data protection principles (see section 3) when accessing, using or disposing of personal information. Failure to observe the data protection principles within this policy may result in disciplinary action up to and including dismissal. For example, if an employee accesses another employee's employment records without the requisite authority, the Rose will treat this as gross misconduct and instigate its disciplinary procedures.

14. International data transfers

The Rose will not transfer personal data to a country or territory outside of the European Economic Area (EEA) unless that country ensures an adequate level of protection for the processing of personal data.

15. Individual rights

As a data subject, employees have a number of rights in relation to their personal data.

Subject access requests

Personnel have the right to make a subject access request. If an individual makes a subject access request, the Rose will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;

- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and
- whether or not the Rose carries out automated decision-making and the logic involved in any such decision-making.

The Rose will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise. If additional copies are required, the Rose may charge an administrative fee.

To make a subject access request, the individual should submit his/her request in writing to the DPT (see section 2). In some cases, we may ask for proof of identification before the request can be processed. The Rose will normally respond to a request within a period of one month from the date it is received. In some cases, and if particularly busy, the Rose reserves the right to extend this period to three months. If a subject access request is manifestly unfounded or excessive, the Rose has no obligation to comply with it.

Other rights
Personnel have a number of other rights in relation to their personal data. They can ask the Rose to:
- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the employee's interests override the Rose's legitimate grounds for processing data (where the Rose relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the Rose's legitimate grounds for processing data.

To ask the Rose to take any of these steps, personnel should send a request in writing to the DPT (see section 2).

If you believe that the Rose has not complied with your data protection rights, you can complain to the Information Commissioner.

16. What if you do not provide personal data?

You have some obligations under your employment contract to provide the Rose with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the Rose with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the Rose to enter a contract of employment with you. If you do not provide other

information, this will hinder the Rose's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

17. Automated decision-making

Employment decisions are not based solely on automated decision-making.

18. Review of procedures and training

The Rose provides training on data protection issues to all personnel who handle personal information in the course of their duties at work, and will continue to provide such individuals with refresher training on a regular basis. Such individuals are also required to have confidentiality clauses in their contracts of employment.

This policy was updated on 16/05/18. The Rose will review and ensure compliance with this policy at regular intervals.