DATA MANAGEMENT POLICY

LEEDS HERITAGE THEATRES

Data Management Policy

1. Introduction:

Leeds Heritage Theatres (LHT) needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Charity's data protection standards – and to comply with the law.

Why this policy exists:

This data management policy ensures LHT:

- Complies with data protection law and follows good practice
- Protects the rights of customers, staff and partners
- Is transparent about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law:

The General Data Protection Regulation (GDPR) applies in the UK and across the EU from May 2018. It requires personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. 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 or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. 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;
5. 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 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 GDPR in order to safeguard the rights and freedoms of individuals;
6. Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
7. The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

2. Who? People and responsibilities

Everyone who works or is associated with LHT contributes to compliance with GDPR. Key decision makers must understand the requirements and accountability of the organisation sufficiently to prioritise and support the implementation of compliance.

- Keeping senior management and board updated about data protection issues, risks and responsibilities
- Documenting, maintaining and developing the organisation's data protection policy and related procedures, in line with agreed schedule
- Embedding ongoing privacy measures into corporate policies and day-to-day activities, throughout the organisation and within each business area that processes personal data. The policies themselves will stand as proof of compliance.
- Dissemination of policy across the organisation, and arranging training and advice for staff
- Dealing with subject access requests, deletion requests and queries from customers, stakeholders and data subjects about data protection related matters
- Checking and approving contracts or agreements with third parties that may handle the Charity's sensitive data
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party services, the Charity is considering using to store or process data, to ensure their compliance with obligations under the regulations
- Developing privacy notices to reflect lawful basis for fair processing, ensuring that intended uses are clearly articulated, and that data subjects understand how they can give or withdraw consent, or else otherwise exercise their rights in relation to the Charities use of their data
- Ensuring that audience development, marketing, fundraising and all other initiatives involving processing personal information and/or contacting individuals abide by the GDPR principles

Data Protection Officer (DPO) – the person responsible for fulfilling the tasks of the DPO in respect of LHT is Amy Sanderson, Head of Communications.

The DPO is responsible for the following;

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc)

3. Scope of personal information to be processed

Please see Appendix 1 for full details.

4. Uses and conditions for processing

Outcome/Use	Processing required	Data to be processed	Conditions for processing	Evidence for lawful basis

Marketing communications (post)	List built based on relevant criteria in ticketing system	Name and address details. History of shows seen	Consent	Evidence of date consent given, how, permitted use and, permitted comms channels.
Marketing communications (email)	List built based on relevant criteria in ticketing system	Name and email address History of shows seen	Consent	Evidence of date consent given, how, permitted use and, permitted comms channels.
Show cancellation or change to ticket/seating	Relevant list of customers to contact	Contact details	Legitimate use	Terms and conditions of sale
Job Applications	Personal Information	Name, address, qualifications, employment history.	Legitimate use	Submitted application form.
Employee personal details	Personal Information	Name, address, DOB, NI number, bank details	Legitimate use	Terms and condition of employment
Employee sickness details	Personal, medical information	Name, address, DOB, payroll number, brief details of illness	Legitimate use	Terms and conditions of employment

5. Privacy Impact Assessments

Privacy impact assessments (PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective PIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

You must carry out a PIA when:

- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.

Processing that is likely to result in a high risk includes (but is not limited to):

- systematic and extensive processing activities, including profiling and where decisions that have legal effects – or similarly significant effects – on individuals.

- large scale processing of special categories of data or personal data relation to criminal convictions or offences.

This includes processing a considerable amount of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to rights and freedoms eg based on the sensitivity of the processing activity.

- large scale, systematic monitoring of public areas (CCTV).

Whilst it is unlikely that personal data stored and processed by LHT will fall under the above definitions of high risk to the rights and freedoms of individuals, we will adopt a best practise approach and a PIA should be completed whenever a project or new initiative outside those already documented in the most recent data audit has implications on the storage or processing of personal data.

What information should the PIA contain?

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.
- A PIA can address more than one project.

Please see Appendix 2 for sample PIA form

6. Data Sharing

Staff

LHT shares staff information with Leeds City Council for the purposes of managing the payroll and the managing attendance policy. There is a Service Level Agreement in place and Appendix 4 shows Leeds City Council's responsibilities and compliance as a Data Processor for this information.

Customers

LHT does not share customer data unless a full data sharing agreement has been signed by both parties and customers have been made aware of what their information will be used for and consented to their information being shared.

We currently have one data sharing agreement in place with Northern Ballet for them to contact customers who have seen their performances at Leeds Grand Theatre with information about other performances in the area.

7. Security measures

All personal information stored by the Charity aside from customer data will be held in LHT Microsoft 365 system meaning it is stored in the cloud on Microsoft servers. Our own server has in place a SonicWall firewall and staff requiring access directly to the server from home

use a secured VPN connection. All access to 365 and the server is password protected and passwords are changed on a monthly basis.

All staff will be issued with the relevant storage protocols including guidance on how long to keep information and how often it should be reviewed.

Using 365 enables access to personal data to be limited to only those who have a business need to see it. This can be changed as the needs of the business change.

Customer data is all stored within our hosted ticketing system, AudienceView. The data is held in a secure UK data centre in Newport and subject to the highest security systems. Only staff who need to be able to view or use customer data have access to that area of the system. All access is password protected with a forced monthly change. Awaiting info from AV around data breaches

8. Automated processing

LHT will use automated processing to analyse customer purchase history including types of performance, booking time, amount spent, seating areas and postcode information to target specific marketing and sales messages and offers. Messages will only be sent when there is consent to do so.

From time to time, we may also use automatic processing for analysis purposes, however, data will be used anonymously in this instance.

9. Subject access requests

All individuals who are the subject of data held by your company are entitled to:

- Ask what information the company holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations

Staff may request copies of information held about them via HR and the form attached in Appendix 3 which will be made available on the staff intranet.

Customers requesting information about data held about them will be asked to fill in a subject access form (Appendix 3) which will then be sent to Amy Sanderson and Rachael Rix-Moore for processing. We will aim to respond to all subject access requests within 15 working days. The legislation states that we must respond within one month. We will not charge a fee for providing this information unless the customer makes repeated requests for the information.

Information regarding customer requests and responses will be stored within AudienceView against the customer record.

10. The right to be forgotten

Customers

Customers have the right to request that we remove their personal data from our ticketing systems.

We will comply with this request once the customer has no outstanding orders with us. We need to hold customer data whilst they have live bookings in order to be able to contact them in the case of a cancellation or change to their tickets.

In deleting personal information, we would still keep the ticket information (seat, performance, price paid) but this would be completely anonymous and no longer attached to the customer.

Staff

Staff records will be held in accordance with the details outlined in Appendix 1 and only deleted before this in exceptional circumstances as this is in the legitimate interests of the Company.

Youth Theatre and Learning Activities

Records of participants will be held and deleted in accordance with the details outlined in Appendix 1.

11. Privacy notices

LHT aims to ensure that individuals are aware that their data is being processed, and that they understand:

- Who is processing their data
- What data is involved
- The purpose for processing that data
- The outcomes of data processing
- How to exercise their rights.

To these ends the company has a privacy statement, setting out how data relating to these individuals is used by the company.

See Appendix 3.

The Privacy Policy can be found on our website and a copy is also available on the staff intranet.

12. Ongoing documentation of measures to ensure compliance

Meeting the obligations of the GDPR to ensure compliance will be an ongoing process. LHT details here the ongoing measures implemented to:

1) Maintain documentation/evidence of the privacy measures implemented and records of compliance.
2) Regularly test the privacy measures implemented and maintain records of the testing and outcomes.
3) Use the results of testing, other audits, or metrics to demonstrate both existing and continuous compliance improvement efforts.
4) Keep records showing training of employees on privacy and data protection matters.

Appendix 1 – Guidance for Storing data

Introduction

Below is a guide advising how data will be stored, who will have access to it and how it will be destroyed, in order to comply with new General Data Protection Regulation from 25th May 2018.

1. Customer Records

How they will be stored?

Customer records will be created, stored and managed within Leeds Grand Theatre & Opera House Ltd ticketing systems, AudienceView (Leeds Grand Theatre and City Varieties) and Jack Row (Hyde Park Picture House)

How long will they be stored?

Customer records will be stored whilst the customer is active (eg continues to attend performances or screenings and/or engage with the Company. The customer has the right to request deletion of their information at any time and this must be carried out in line with the GDPR.

If a customer has become inactive, moved away without informing us or deceased, the information will be deleted following review every 5 years.

How will the details be destroyed?

Identifying customer information will be removed from the database

Who will have access?

At Leeds Grand Theatre and City Varieties, Box Office staff, Communications staff and Duty Managers all have access to customer data as do key members of the Learning Team. Anyone wishing to access the system must have a username and a secure password which is changed monthly. The system can only be accessed via a secure, static IP address which is only allowed through the firewall if permission is given via a System Administrator.

System administrators can view every user interaction with a customer records through the Audit function.

Access will be reviewed on a two monthly basis to ensure that anyone who no longer needs access has their account deleted.

2. Job Applications

How they will be stored?

Job applications received via email to the HR manager will be saved to the HR area in Office 365 along with the shortlisting records and interview notes.

How long will they be stored?

Candidates have the right to access any data the company holds on their application; therefore, HR will retain all these documents for 6 months.

How will the details be destroyed?

After 6 months the relevant file on Office 365 will be deleted by the HR Manager or Head of Support Services, and any paper copies of applications and interview notes held by HR Manager will also be destroyed via confidential shredding.

All job applications received via email to the recruiting manager should be saved to the relevant HR section in Office 365 and then the email deleted from their inbox and also from their deleted items. Alternatively remove the attachment from the email in your inbox.

Who will have access?

The HR Manager and Head of Support Services will have full un-restricted access to the job applications saved in the HR area of Office 365. The recruiting manager will have access only to the relevant job applications that they are dealing with. This will be managed and controlled by the Head of Support Services via the permissions and granted access within Office 365.

3. Disciplinaries & Grievances

How they will be stored?

Disciplinary and Grievances will be save to the HR area in Office 365 along with all relating correspondence such as letter to the employee and notes of meetings. A paper copy of the outcome letter will also be saved in the employees personal file which is retained in a secure locked office with restricted access to files to only the HR Manager and Head of Support Services.

How long will they be stored?

A copy of the outcome from any disciplinary or grievance will remain on an employee's file throughout their employment and seven years after they have left the company. The information stored in the HR section of Office 365 will be deleted two years after the conclusion of the disciplinary or grievance.

Although the outcome of a disciplinary will be stored in an employee's personnel files, most warnings will be disregarded for disciplinary purposes after a specific period (e.g. 6 months for a verbal warning, 12 months for a final written warning) subject to satisfactory conduct and performance.

How will the details be destroyed?

Seven years after the termination of an employee's employment their personnel files and all related data will be destroyed in confidential waste. Any disciplinaries or grievances stored in the HR section in Office 365 will be deleted two years after the conclusion of the disciplinary or grievance.

Who will have access?

The HR Manager and Head of Support Services will have full un-restricted access to disciplinary and grievance records stored in HR area of Office 365. The relevant managers involved in undertaking the disciplinary investigation and disciplinary hearings or grievances will have access only to the relevant cases that they are dealing with. This will be managed and controlled by the Head of Support Services via the permissions and granted access to files within Office 365.

4. New employee Info

Upon joining the company, employees will be asked to complete number of forms which are required to set them up on the Leeds City Council payroll system (as the LGT&OH Ltd does not have its own payroll function), these forms will require personal data to be provided (name, address, date of birth, national insurance number, bank details) and a copy of ID such as passport or driving licence to prove right to work in UK.

How they will be stored?

These forms will then be retained on an employee's personnel file in a secure and locked office. The forms will also be shared with Leeds City Council (LCC) due to us using their payroll system. The HR Manager will send these forms electronically to LCC who will use them to create your profile on their payroll system, these emails will then be deleted by LCC.

How long will they be stored?

Throughout your employment and for a period of seven years after termination of your employment, the Company will need to process data about you for purposes connected with your employment. After seven years the data will be destroyed in confidential waste.

How will the details be destroyed?

Personnel files following termination of employment are stored in a secure locked room with restricted access to HR and Finance. At the end of each financial year the HR Manager will arrange the confidential disposal of files older than 7 years.

Who will have access?

Employee personnel files are retained in a locked office with restricted access to the files to only HR manager and Head of Support Services. Employee files can also be accessed by an employee's line manager as required.

5. Sickness and Holiday Records

How they will be stored?

Employee's holidays and sickness are recorded using BrightHR. Sickness will be recorded by the HR Manager in BrightHR and with LCC, Holiday's will be requested through the system by employees. Individual line managers may also keep their own record of their department's sickness and holidays.

Forms completed by employees and line managers such as return to work interviews, special leave requests, fit notes are all stored in an employee's personnel file on BrightHR.

How long will they be stored?

Throughout your employment and for a period of seven years after termination of your employment, the Company will need to process data about you for purposes connected with your employment. Therefore, after seven years the employees personnel file will be destroyed in confidential waste.

How will the details be destroyed?

Personnel files following termination of employments are stored in a secure locked room with restricted access to HR and Finance. At the end of each financial year the HR Manager will arrange the confidential disposal of files older than 7 years old. Electronic files will follow the same disposal time period.

Who will have access?

Employee personnel files hard and/or electronic are retained in a locked office with restricted access to the files through Office 365 and BrightHR to only HR manager and Head of Support Services. Employee files both hard and electronic can also be accessed by an employee's line manager as required.

GDPR – Learning Information

Guidance for Storing Data

1. Introduction

Below is a guide advising how Learning related data will be stored, who will have access to it and how it will be destroyed, in order to comply with new General Data Protection Regulation from 25th May 2018.

2. Consent Forms:

Including emergency contact details, date of birth, medical/access info, photo permissions

How they will be stored?

Consent forms for Learning Projects, workshops and photo permissions (including Youth Theatre, LAIT, Summer Festival, work experience and volunteers), received via email to the lead Learning Team member will be saved to the Learning TEAMs Personal Data area in Office 365. Paper consent forms will be scanned and saved to this area.

Paper copies will only be kept if they are needed on hand during the workshop for the safety of or to safeguard participants. When necessary, the lead Learning Team member will keep the details secure and on their person and destroy them at the end of the project. For ongoing projects such as youth theatre, the emergency contact details are kept locked in the laptop cabinet within the Learning Suite cupboard.

How long will they be stored?

The Learning Team will keep the above details for the duration of the project to enable participants to safely engage with the activities.

Photo consent forms will be kept for 5 years along with the relevant images.

How will the details be destroyed?

Consent forms and applications will be deleted at the end of projects. An annual review of the consent/application files kept on the Learning area of Office 365 will take place once a year to review this process and appropriate files will be deleted.

Consent forms/applications for ongoing projects will be retained for the duration of the engagement. Forms will be deleted when members leave the project. An annual review of the consent/application files kept on the Learning area of Office 365 will take place once a year and appropriate files will be deleted.

Photo consent forms and images will be deleted from the Learning area of Office 365 after 5 years and will not be used in additional print.

Who will have access?

The Learning Team will have full access to consent forms saved in the Learning area of Office 365. Digital documents are also further protected by a password. This will be managed and controlled by the Head of Learning via the permissions and granted access within Office 365.

3. Work Experience, Learning Volunteer and freelance Applications:

Including emergency contact details, date of birth, medical/access info, photo permission

How they will be stored?

Application forms for work experience, learning volunteers and learning freelancers, received via email to the Learning Team, will be saved to the Learning TEAMS Personal Data area in Office 365.

How long will they be stored?

Application forms will be kept for the duration of the work experience and/or volunteering position. Unsuccessful applications will be kept for up to 12months as future positions may become available.

How will the details be destroyed?

After 12 months the relevant files on Office 365 will be deleted by the lead project member of the Learning team.

All work experience and Learning Volunteer applications received via email to the Learning Team should be saved to the relevant Learning section in Office 365 and then the email deleted from inboxes and deleted items. Alternatively the attachments will be deleted from the email in inboxes.

Who will have access?

The Learning Team will have access to the application forms to aid supervision and the safeguarding of participants.

4. Freelance Agreements:

Including addresses, phone numbers, National Insurance number, DBS certificate number

How they will be stored?

Completed freelance agreements for Learning activities, received via email to the Learning Team, will be saved to the Learning TEAMS Personal Data area in Office 365.

Paper freelance agreements will be scanned and saved to this area and one copy provided to the Head of Finance who will keep them in their secure office for auditing purposes.

How long will they be stored?

Freelance agreements will be kept by the Learning Team for the duration of the commissioned work or whilst the freelancers are still working in partnership with the Company.

The Head of Finance will retain a copy of the freelance agreements for a duration of 7 years in line with our financial regulations.

How will the details be destroyed?

On the completion of the commissioned work the freelance agreements will be deleted from Office 365 by the lead project member of the Learning team. This will be reviewed on an annual basis to ensure relevant agreements have been deleted.

All freelance agreements received via email to the Learning Team should be saved to the relevant Learning section in Office 365 and then the email deleted from inboxes and deleted items. Alternatively the attachments will be deleted from the email in inboxes.

The Head of Finance will delete the paper copy of the agreements after 7 years

Who will have access?

The Learning Team will have access to the agreements to support the management and supervision of the freelancers. The Head of Finance will also have access to the agreements for auditing purposes.

5. DBS checks and associated risk assessments:

How they will be stored?

DBS checks are completed online through Leeds City Council's DBS portal and therefore once inputted, personal information is not kept or stored by the Company.

Once completed the Company will complete a visual check of the DBS certificate but not retain any copies. Only a copy of the DBS certificate number and issue date is stored on the HR TEAMS area in 365 in the Training Register.

If disclosures are made to the Company following a DBS check then a risk assessment will document control measures put in place to mitigate any risks. Such risk assessments will be password protected and saved on the HR TEAMs area in Office 365.

How long will they be stored?

DBS certificate numbers and issue dates and any associated risk assessments will be stored in the HR area of Office 365 for the duration of employment (including volunteering placements) or commissioned activities.

How will the details be destroyed?

On an annual basis the DBS information included in the training register reviewed and associated risk assessments will be reviewed by the Head of Learning. Information will be deleted when employees no longer work for the Company or when volunteers/freelancers have completed their placements/commission.

Who will have access?

SMT have access to the Training Register stored in the HR area of Office 365 which will contain certificate numbers and issue dates of DBS checks. However, if disclosures are made via Leeds City

Council's online portal as the registered body, a risk assessment will be produced by the Head of Learning and stored in the HR area of Office 365 with password protection. The risk assessment will be shared on a need-to-know basis only with the Learning Team in order to safeguard participants and staff.

6. Safeguarding concerns and disclosures:

How they will be stored?

The Designated Safeguarding Officers (DSOs) for the Company will obtain and keep on record information regarding safeguarding concerns and disclosures using the Company's template reporting form at appendix 2 of the Company's Safeguarding Policy. The forms will be stored in Office 365 in the Learning area. The information will be password protected and any paper copies will be scanned and uploaded to this area.

How long will they be stored?

Safeguarding concerns and disclosures will be retained for the duration of engagement between the child/vulnerable adult and the Company.

How will the details be destroyed?

On an annual basis the safeguarding concerns folder in Office 365 in the Learning area will be reviewed by the Designated Safeguarding Lead. Concerns and disclosures will be deleted once participants are no longer engaged with activities at the Company.

Who will have access?

The DSOs will have access to the forms that capture concerns/disclosures to aid the monitoring and processing and reporting of safeguarding concerns, liaising with the Local Authority Duty and Advice Team, social services and the police where necessary. This will be managed and controlled by the Head of Learning via the permissions and granted access within Office 365.

Information about a child or vulnerable adult presenting immediate and significant risk of harm to themselves or others will be communicated to relevant staff on a need to know basis only, in line with our safeguarding policy.

7. Child Performance Licenses:

Name, address, school, date of birth

How they will be stored?

To apply for child performance licenses, information regarding performers name, age, school and address will be inputted to the child performance applications and Body of persons license application and sent to Leeds City Council as licensing body. Applications will be deleted after the performance has taken place with the exception of youth theatre which will be stored for a period of 12months to cover multiple performances. The application forms will be saved in Office 365 in the Learning Area with a password protection.

How long will they be stored?

Until the completion of the performance excepting youth theatre which will be stored for a period of 12 months to cover multiple performances.

How will the details be destroyed?

The Learning Team Project Manager will delete the applications as per the timescales above. On an annual basis the personal data in Office 365 in the Learning area will be reviewed by the Head of Learning.

Who will have access?

The Learning Team will have access to the application form to aid the running of performances. This will be managed and controlled by the Head of Learning via the permissions and granted access within Office 365.

8. Tour and Workshop Booking Forms: Including names, addresses, phone numbers and email addresses

How they will be stored?

Completed booking forms for tours and workshops will be saved to the Learning TEAMs Tours and Workshop Bookings channel in Office 365.

How long will they be stored?

Completed booking forms will be kept for no longer than one month after the tour/workshop has taken place.

How will the details be destroyed?

Completed booking forms pertaining to tours/workshops that have taken place will be deleted on a monthly basis by the Learning Team. Copies of booking forms sent to bookers will be deleted from Sent folders and Deleted Items folders.

Who will have access?

The Learning Team will have access to Tours and Workshop Booking Forms in the Tours and Workshop Bookings channel to enable effective delivery of tour and workshop activity.

Privacy impact assessment screening questions

These questions are intended to help you decide whether a PIA is necessary. Answering ‘yes’ to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

Will the project involve the collection of new information about individuals?

Will the project compel individuals to provide information about themselves?

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.

Will the project require you to contact individuals in ways that they may find intrusive?

Privacy impact assessment template

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA.

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Annex three can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (eg the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns

Privacy policy

This privacy policy sets out how Leeds Heritage Theatres (LHT) uses and protects any information that you give LHT when you use this website.

LHT is committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when using this website, then you can be assured that it will only be used in accordance with this privacy statement.

LHT may change this policy from time to time by updating this page. You should check this page from time to time to ensure that you are happy with any changes. This policy is effective from May 2018.

What information do we collect?

If you are a visitor to the website and are merely visiting public areas for information purposes, we will not collect any personal data from you. However, in the background we may automatically collect information about your visits and pages you have visited. This Information does not reveal any of your Personal Data and is only used in aggregate for analysis, management and development of www.leedsheritagetheatres.com

Controlling your personal information

In order to make a purchase via our website, we ask that you create an account using your email address as a username. This enables us to ensure we can contact you regarding any issues or changes to your booking. It also helps us limit the duplication of information about you on our system.

You may choose to restrict the collection or use of your personal information in the following ways at any time via the Your Account section of our website or by emailing info@leedsgrandtheatre.com:

1. By telling us which information (if any) you would like to receive from us
2. By telling us the channels you are happy for us to contact you on
3. By letting us know any changes to your information either by amending in your online account or telling us in person, by email or on the telephone
4. By asking us to delete your information at any time

We will not sell, distribute or lease your personal information to third parties unless we have your permission to do so.

You may request details of personal information which we hold about you under the General Data Protection Regulation 2018.

Security

We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online.

While we cannot guarantee the security of the Internet, this website has security measures in place to protect against the loss, misuse and alteration of the information you provide us. Our secure server software (SSL) is the industry standard and among the best software available today for secure online transactions. It encrypts all of your personal information, including credit card number, name and address so that it cannot be read as the information travels over the Internet.

How we use cookies

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added, and the cookie helps analyse web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

We use traffic log cookies to identify which pages are being used. This helps us analyse data about web page traffic and improve our website in order to tailor it to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website, by enabling us to monitor which pages you find useful and which you do not. A cookie in no way gives us access to your computer or any information about you, other than the data you choose to share with us.

You can choose to accept or decline cookies. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

Links to other websites

Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

Business Support Centre
St George House
40 Great George Street
Leeds
LS1 3DL

21 May 2018

General Data Protection Regulations (GDPR) – Leeds City Council acting as a data processor

As you may know, new data protection legislation is due to come into force in the UK during May 2018, which aims to protect the privacy of all EU citizens and prevent data breaches. It will apply to any public or private organisation processing personal data.

Established key principles of data privacy will remain relevant in the new Data Protection Legislation, but there are also a number of changes that will affect commercial arrangements, both new and existing, with our customers. The new GDPR specifies that any processing of personal data by a processor should be governed by a contract with certain provisions included.

We are mindful that we have contractual obligations to you as a valued customer in relation to the processing of personal data, and this letter is to highlight how we propose to deal with the GDPR from 25 May 2018. The Council, as a data processor will meet the terms as described in Appendix 1 attached to this letter below.

If you have any questions or feel it necessary to change any of the clauses described below, please contact by email at BSCTrainingandComms@leeds.gov.uk or, if you would like to know more about the upcoming changes, the Information Commissioner's Office is a useful source of information on the new regulations.

Yours faithfully

Helena Phillips
Chief Officer, Shared Services

APPENDIX 1

GDPR Definitions

"**Data Controller**", "**Processor**", "**Data Subject**", "**Personal Data**", and "**Processing**" shall have the meanings prescribed under the Regulation;

"**Regulation**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation);

Clauses

When processing your personal data-

1.1 The Parties acknowledge that the Council may have access to your Personal Data. Where this is the case, you as the Controller of such Personal Data appoints the Council as its Processor to process such Personal Data on your behalf.

1.2. You warrants that the processing by the Council of the Personal Data is authorised by the relevant Controller.

1.3 The Council agrees that it will implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of the Regulation and ensure the protection of the rights of Data Subjects and in particular the Council will implement any specific measures set out in Schedule 1 of this Agreement.

1.4 The Council will not engage another Processor without prior specific written authorisation from you, such authorisation not to be unreasonably withheld or delayed, and it shall be deemed to be reasonable for you to withhold such authorisation unless and until such other Processor shall have entered into a binding agreement with the Council whereby such other Processor agrees to observe and perform the same obligations as regards compliance with the Regulation as are imposed upon the Council by this Clause 1. Notwithstanding the completion of such binding agreement, the Council will remain fully liable to you for any breach, non-performance or non-observance of this Clause 1 by such other Processor in the same way and to the same extent as if such breach, non-performance or non-observance had been committed by the Council.

1.5 The Council will Process Personal Data in accordance with Schedule 1 of this Agreement, and in accordance with any written instructions by you. Such instructions will include your requirements with regard to transfers of Personal Data to a third country or an international organisation by the Council, unless the Council is required to do so by law, and in such a case the Council shall inform you of that legal requirement before processing unless prohibited by law on important grounds of public interest. The Council shall immediately inform you if, in its opinion, any such instruction by you infringes the Regulation.

1.6 The Council will ensure that all persons authorised or permitted by the Council to Process Personal Data have committed themselves to confidentiality.

1.7 The Council will take all measures required pursuant to Article 32 of the Regulation, and in particular will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

1.8 The Council will provide all reasonable assistance to you by taking appropriate technical and organisational measures, insofar as is possible, for the fulfilment of your obligations to respond to requests for exercising Data Subjects' rights laid down in Chapter III of the Regulation.

1.9 The Council will provide all reasonable assistance to you in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the Regulation taking into account the nature of the Processing and the information available to the Council.

1.10 The Council will at your direction and discretion delete, or return to you all Personal Data upon the expiry or other termination of your Agreement with the Council, and the Council will delete any copy of such Personal Data unless required by law to continue to store such Personal Data.

1.11 The Council will make available to you upon demand all information which is reasonably necessary to demonstrate compliance with the obligations laid down in Article 28 of the Regulation, and will permit and contribute to audits, including inspections, conducted by you or another auditor mandated by you for such purposes.

1.12 The Council will maintain a record of all categories of Processing activities carried out on your behalf in accordance with Article 30.

1.13 You acknowledges that it is your responsibility to comply with the Regulation in respect of the personal data, as defined under the Regulation, which you hold and shall indemnify the Council in respect of any claims by any person or body in respect of your responsibilities under the Regulation.

Schedule 1

Please refer to your Service Level Agreement for payroll, pensions, HR administration and central payments services.