



Full House Theatre Data Protection Policy

Key details:

- Approved by board: April 2025
- Policy became operational on: April 2025
- Next review date: April 2026

1. Context and overview

Full House needs to gather and use certain information about individuals. It collects information about the number of participants, their ages, gender, ethnicity and addresses including postcodes, together with verbal and written feedback from both adults and children for funding purposes. It also collects names and email addresses to send out our e-newsletter about our projects and shows.

Other data held by the company includes customers, suppliers, business contacts and employee details.

This policy describes how this personal data is collected, handled and stored to meet the company's data protection standards and to comply with the law.

Why this policy exists:

This data management policy ensures Full House Theatre:

- 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 and is monitored by The Information Commissioner's Office <https://ico.org.uk/>.

This will stand prior to revised GDPR being fully launched in the UK at which point this Policy will be up-dated accordingly. 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 be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals;
6. Processed and held 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.
8. Data is not transferred outside the countries of the European Economic Area without adequate protection.

Areas of allowable data storage

- Performance of a contract
- To comply with the law
- Vital Interest – to save a life
- Public Task – to perform a task in the public's interest
- Legitimate Interest – necessary for your work

People and responsibilities

Everyone at Full House Theatre works to comply with General Data Protection Regulations (GDPR) in order to prioritise and support the implementation of compliance.

The Data Protection Officer (DPO) is Harriet Hardie , harriet@fullhouse.org.uk who has sole responsibility and access to any stored data. The DPO has regular training relating to data protection. The Data Protection and Privacy policies and procedural information is disseminated within the team.

The DPO's responsibilities include (but are not necessarily limited to):

- 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 unit 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 clients, stakeholders and data subjects about data protection related matters
- Checking and approving contracts or agreements with third parties that may handle the company'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 company 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 company's 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
- 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)
- To ensure no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party
- To ensure personal data is kept in accordance with Full House Theatre's retention schedule (7 years or less)

Staff members should:-

- promptly direct any queries regarding data protection, including subject access requests and complaints to the DPO
- swiftly bring any data protection breaches to the attention of the DPO and support the DPO in resolving breaches. If any breach is dangerous or compromising for any individual, reported to Information Commissioners Office (ICO) <https://ico.org.uk/> within 72 hours
- Seek advice from the DPO where there is uncertainty around a data protection matter

Contractors, Short-Term and Voluntary Staff

All practical and reasonable steps are taken to ensure that contractors, short-term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

The DPO is responsible for the use made of personal data by anyone working on the company's behalf. Any contractors, short-term or voluntary staff must be appropriately vetted by the DPO and ensure that:

- any personal data collected or processed in the course of work undertaken for Full House Theatre is kept securely and confidentially
- all personal data is returned to the DPO on completion of the work, including any copies that may have been made. Alternatively, that the data is securely destroyed and Full House Theatre receives notification in this regard from the contractor or short-term/voluntary member of staff

2. Scope of personal information to be processed

Full House Theatre is committed to the principals of Data Protection and Article 5 under General Data Protection Regulation.

Type of Data	Personal Data
Description of data	<p>Names, postal addresses, email addresses, age, gender, ethnicity, verbal and written feedback forms and photo consent of participants, audiences, supporters, subscribers.</p> <p>Salaries, bank details, contracts, payroll, performance management of employees and staff.</p>
Person responsible	Harriet Hardie (Data Controller)
Date of consent to hold data	When obtained from the individual.
Where the data is stored	Barracuda, Office 365, MailChimp, Eventbrite, Google Analytics and Facebook. Office computers / laptops. Full House office.
Source of the data	Booking forms (workshops), online sign up forms (MailChimp & Website), online bookings (Eventbrite & Ticket Tailor), Emails, Feedback / Evaluation forms, Facebook Adverts.
Purpose of the data	<p>Communication with individuals about Full House projects, workshops, events, shows and publicity / marketing.</p> <p>Essential personal data required for processing payroll, issuing contracts.</p>
How the data is protected in its storage	<p>Security systems maintained by third parties; MailChimp, Eventbrite, SAGE, Ticket Tailor, Barracuda Software, Office 365, Google Analytics and Facebook.</p> <p>Office computers and laptops are all password protected. Hard copies are kept in a locked filing cabinet. Only the DPO has access to the key.</p>

Usage restrictions	Only employees with express permission can access and process payroll.
Retention period	All information to be held securely for up to 7 years. At the 7 year point, we follow the delete data procedure to ensure destruction of data is thoroughly completed.
Comments	Individuals have the right to erasure and can request this at any time.

This information audit was completed in April 2025. It may be updated to take into account changes at Full House Theatre or to reflect changes to regulation or legislation.

3. Uses and conditions for processing

Outcome/Use	Processing required	Data to be processed	Conditions for processing	Evidence for lawful basis
To inform future programming and funders	Printed forms and MailChimp. Password protection on office computers. MailChimp – see below.	Feedback forms	Consent	Evidence of date consent given, how, and permitted use.
Distribution of e-newsletter and publicity material	<i>MailChimp</i> . Click here for MailChimp privacy policy https://www.intuit.com/privacy/statement/	Names, email and postal address	Consent, refreshed every 5 years	Evidence of date consent given, how, and permitted use
Promotion, reporting, sales, alerts.	Eventbrite Click here for Eventbrite privacy policy https://www.eventbrite.com/help/en-us/articles/460838/eventbrite-privacy-policy/ Ticket Tailor Click here for Ticket Tailor privacy policy	Names, postal and email address, photo consent	Consent	Evidence of date consent given, how, and permitted use

	https://www.tickettailor.com/legal/privacy-policy Further GDPR information for Ticket Tailor can be found here https://www.tickettailor.com/legal/gdpr			
Promotion and reporting	Google Analytics anonymous collection of information. Click here for Google opt out and privacy policy. https://policies.google.com/privacy?hl=en Full House cookies policy https://fullhouse.org.uk/wp-content/uploads/2023/11/Full-House-Theatre-Cookie-Policy-2.pdf	Information on how visitors use the website	Cookies consent	Relevant policies and procedures in place
Helps us understand user behaviour on Facebook and website	Website / Facebook Click here for Facebook privacy policy https://www.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0	Identify anonymous users from Facebook ads	Cookies consent	Relevant policies and procedures in place
For employment, promotion, sales, fundraising, reporting.	Microsoft Office 365, SAGE and Barracuda Software	Personal data	Password protection	Data protection and privacy policies procedures
Fundraising, reporting	Microsoft Office 365 and Barracuda Software	Name, address, age, ethnicity and gender	Password protection	Evidence of date consent given, how, and permitted use.

Processing Sensitive Information

Sometimes it is necessary to process sensitive personal information. This may be to ensure Full House Theatre is a safe place for everyone. It may also ask for information about particular health needs, such as allergies to particular forms of medication, or any health conditions or disabilities. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and participants will be asked to give express consent for Full House Theatre to process this information, with detail of how and with whom the information may be shared with detail of entitlement to withdraw consent at any time.

(See [Appendix two Privacy Policy](#))

Categories of sensitive personal data:

- a. racial or ethnic origin
- b. political opinions
- c. religious beliefs or other beliefs of a similar nature,
- d. trade union membership
- e. physical or mental health
- f. sexual
- g. commission or alleged commission of any offence, or
- h. any 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.

4. Privacy Impact Assessments

Privacy Impact Assessments (PIAs - also known as Data Protection Impact Assessments, DPIAs) will be undertaken as a way to help us identify the most effective way to comply with our data protection obligations and meet individuals' expectations of privacy, and protect against the risk of harm through use or misuse of personal information. It will allow Full House Theatre to identify and fix problems at an early stage.

(See Appendix One)

5. Data Sharing

Third-Party Data Processors

Where external companies or individuals are used to process personal data on behalf of Full House Theatre:

- a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
- reasonable steps will be taken that such security measures are in place.

Individual consent is the basis for sharing data. Full House Theatre will obtain and record the necessary specific, clear, granular permissions for sharing data with NAMED third parties, stating specifically defined uses, specified communications channels, defining the scope of the personal data to be shared. Such data will be shared securely by way of the DPO in a form that can facilitate a data subject access request. The DPO will establish the understanding of the receiving organisations' or individual's obligations as a data controller with responsibility for all aspects of the regulation as data controllers of the new copy of the data which is being shared with them in compliance with the Full House Theatre's Data Protection and Privacy policies.

6. Security measures

Full House Theatre restricts and protects access to data to those people for whom it is necessary to perform the processing. It uses security software (Barracuda), Norton and password protection. Please see [Appendix Two](#) for Full House Theatre Privacy Policy and [Point 4](#) for relevant users Privacy Policies. For deletion protocol, please see [Point 11](#).

There are protocols in place for safe transfer of data in transit, and protocols for password management and data back-up. Please see [Appendix Three](#) for **Data Breach policy and protocol**. Any breaches are reported to the ICO within 72 hrs of any breach becoming known, by the DPO.

7. Subject access requests

All individuals who are the subject of data held by Full House Theatre 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

Details of how an individual can access their stored data are outlined in the Privacy Policy, including the right to be forgotten. ([See Appendix Two](#))

8. Privacy notices

Full House Theatre 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 Policy, setting out how data relating to these individuals is used by the company. ([See Appendix Two](#))

9. Delete Data Procedure

The deletion of personal data is an important activity in data protection, given the fifth data protection principle's requirement that "personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes".

Equipment

It's important to properly delete any personal information before selling or disposing of hardware, so that it cannot be accessed by anybody else either by mistake or for malicious purposes.

Personal data can be stored on any device with a permanent memory, including desktop and laptop computers, external hard drives, mobile phones, tablets, printers, and removable memory such as that found in digital cameras.

Methods of destruction

A variety of methods should be employed to ensure all data records are adequately destroyed. These are; physical destruction, secure deletion software, restoring factory settings, formatting or send to a

specialist. The DPO will contact the cloud provider to see what service they offer to securely delete data as required.

Communication and Timescales

Individuals can make a request for erasure verbally or in writing. If a verbal request is made, this is internally documented in writing by the DPO.

The individual will be contacted to confirm the actions taken by the company, being absolutely clear to individuals what it means by deletion and what actually happens to personal data once the company has deleted it. Full House Theatre has one month to respond to a request. Information requested to be deleted may need to be retained for HMRC purposes. (*See Putting information 'beyond use' below*).

Procedure

- Request for erasure identified
- Confirmation of ID obtained from individual to validate request
- Request acknowledged in writing explaining the implications and sent to individual
- Request logged by Full House Theatre with one month deadline
- All relevant personal data identified
- Delete data plan put in place with details of how and when will this be done and by whom
- Cross check of identified data with Data Controller Harriet Hardie
- Personal data destroyed
- Email sent to individual to confirm actions

Putting information 'beyond use'

If it is not possible for the data to be deleted, the DPO will ensure that all four of the following are in place:

- DPO is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
- does not give any other organisation access to the personal data;
- surrounds the personal data with appropriate technical and organisational security; and
- commits to permanent deletion of the information if, or when, this becomes possible.

In the event that personal data to be deleted has been disclosed to others or made public in an online environment (for example on social networks, forums or websites) the DPO will contact each recipient and inform them of the erasure, (unless this proves impossible or involves disproportionate effort).

10. Ongoing documentation of measures to ensure compliance

Meeting the obligations of the GDPR to ensure compliance will be an ongoing process. Full House Theatre 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 the DPO and employees on privacy and data protection matters.

- 5) The Board of Trustees will review the Data Protection and Privacy Policies every year, or earlier in the event of any law changes that may affect the policies.

Appendix 1

Privacy Impact Assessments (PIA's) / Data Protection Impact Assessments, (DPIA's) Process

What data do we collect?

(Name, email address, social media posts, location, IP address, Cookies)

Where do we store the data?

(Emails, documents, databases, backups, email lists)

How do we protect and document the data we have?

(Passwords, limited access, databases)

How long do we plan to keep the data for?

(Three Years, Five Years seven years, etc...)

Do we have a function/ reason for the data we collect?

Legitimate interest, etc.

Process in relation to the purpose

Necessity and proportionality

An assessment of the risks to individuals

Level of risk through any data breach and measures in place to address the risk, including security

What is the process if someone asks to be removed from our records?

(Whose responsibility, what records needs to be checked etc...)

Appendix Two

Full House Theatre Privacy Policy

1. Purpose of our Privacy Statement

Under the UK General Data Protection Regulation, we are required to explain to you why we ask for personal data about you, how we intend to use the information you provide and whether we will share this with anyone else.

2. Who are we?

Full House Theatre is a registered Charity Incorporated Organisation (ICO) number 1165541, registered address: 12 Kings Arms Yard, Church Street, Ampthill, Bedfordshire, MK45 2PJ.

For further information about ICO's <https://www.gov.uk/government/publications/charitable-incorporated-organisations/practice-guide-14a-charitable-incorporated-organisations>

Our vision is for every child to hold treasured memories of theatre. With our audience at the heart of our work, we carefully craft, programme and develop theatre and performance projects for, by and with children and young people. We exist to enrich young creative minds, delight young audiences, and nurture a lifelong connection with the arts.

Full House is committed to listening and responding to the needs of our audience, reaching out to all corners of the community to create lasting memories.

3. How to contact us

If you have any concerns or questions about our use of your personal data, you can contact us by writing to Full House Theatre, 12 Kings Arms Yard, Church Street, Ampthill, Bedfordshire, MK45 2PJ or info@fullhouse.org.uk or call 01525 630783.

To opt out from receiving information from us, please email your full name and postcode to info@fullhouse.org.uk with "Opt-Out" in the subject line. We will process your request within 5 working days and ensure that your data is removed from our records. We will also ask any partners we have shared your data with (with your permission) to do the same.

If you receive our e-newsletter you can amend your personal details and email contact preferences at any time. Simply click on the links provided in the footer of the e-newsletter to unsubscribe or update your preferences.

You also have the right to complain to the Information Commissioner's Office (the "ICO") if you are

not satisfied with the way we use your information. You can contact the ICO by writing to Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

4. Why are we collecting your information?

We collect information about you when you fill in our feedback cards after shows, sign up to email updates on <https://fullhouse.org.uk>, leave comments on our website or opt in to partner venues sharing your data with us. We use this to supply you with the latest information about Full House Theatre, keep in touch with you and let you know about future performances, workshops and events. We also use your information for our own marketing and fundraising purposes (e.g. audience segmentation) to meet our requirements to use our charitable resources effectively, report to our funders and to offer you a better experience. We may also collect information on your needs, ethnicity, age and gender so that we can make our performances and workshops more accessible and inclusive.

5. What information are we collecting?

The only information we collect about you is the information that you provide to us via cookie tracking, email sign up, comments and enquiry forms on our website or when filling in feedback forms after performances or workshops. We may also collect information about you through online/offline surveys, email lists from venues and social media interactions.

Some of the information which we collect will be special categories of personal data (also called sensitive personal data), which includes information about your age, disability and racial or ethnic origin. This is collected for us to monitor how diverse and inclusive we are as an organisation and to make our future performances or workshops more accessible and inclusive. It also helps us provide better and more tailored audience experiences, better reflecting your needs. By providing us with this information, you consent to our use of this information for this purpose.

With your consent, Full House Theatre collects and retains photograph's and videos of participants and audiences during performances and workshops for use in printed and online publicity, social media, press releases and funding applications and reports.

6. What we are going to do with your information

The information you provide to us will be used for the following purposes:

- It will be stored and used by us in accordance with this privacy statement and also in accordance with your rights under the General Data Protection Regulation (UK GDPR)
- It will be collected and used by us fairly and openly for the purpose of marketing and evaluation
- It will allow us to provide communications, workshops, shows and other services which are tailored to your needs

- It will allow us to make contact with you in the most appropriate way. For example, we can provide visual stories for people with accessible learning needs; or in an alternative language if English is not your first language.

7. What is the legal basis for using your information?

In accordance with the data protection laws, we need a "legal basis" for collecting and using information about you. There are a variety of different legal basis for processing personal data which are set out in the data protection laws.

The lawful basis on which we rely in order to use the information which we collect about you for the purposes set out in this notice will be:

- you have provided consent to our use of your information; and
- using your information is necessary for us to comply with a legal obligation to which we are subject.

The lawful basis on which we rely in order to use your special categories of personal data which we collect about you, is that you have provided your explicit consent to our use of your information.

8. Sharing your information

It may be necessary to share information about you with our contractors and sub-contractors in order to provide you with the services in accordance with the contract between us. We will only share information about you with the contractors and sub-contractors which is relevant and necessary to address your individual needs. The contractors and sub-contractors shall be contractually required to ensure that they adhere to the security requirements imposed by the UK General Data Protection Regulations (as applicable). Our contractors and sub-contractors will not share your information with any other parties and will only be able to use the information when completing work on behalf of Full House Theatre.

We may also be required to share your information with our regulators (such as the Charities Commission), who have permitted access to this information by law, and with other organisations with whom there is a legal obligation to share information. We also share information with our funders (such as Arts Council England) in order to meet contractual obligations.

We may, from time to time, share your information with other organisations, such as theatres and other venues. This includes information provided on feedback cards and surveys which may include email addresses, name, event attended and other information that you have completed and agreed for us to share with third parties for marketing and promotional purposes.

9. Cookie Statement

Full House Theatre website uses cookies. This statement explains what cookies are and why we use them. Full House cookies policy <https://fullhouse.org.uk/wp-content/uploads/2023/11/Full-House-Theatre-Cookie-Policy-2.pdf>

What are cookies?

Cookies are small data files that are stored on your computer or mobile device when you visit a website. Cookies are widely used by online service providers in order to e.g. make their websites or services work. The cookies we use on our website won't collect personal, identifiable information about you and we won't disclose information stored in cookies that we place on your device, to third parties. The cookies we send to your device only relate to your use of our website; they don't have any other effect on your device.

Full House Theatre collects anonymous information about those who visit our website via Google Analytics and Facebook. Clear instructions to opt out are provided.

Cookies from third party websites

A limited number of pages on our website use content embedded from third party websites. These third-party websites may send cookies to your device. We encourage you to read the privacy statements on the other websites you visit. In addition, if you are linked to our website from a third party site, we cannot be responsible for the privacy policies and practices of the owners and operators of that third party site and recommend that you check the policy of that third party. You can opt out of these by using the Cookie Consent pop-up on entry to the website.

10. Transferring your information abroad

We will not transfer the information you provide to us outside of the European Economic Area.

11. Security of your information

The information that you provide will be stored securely on our systems and if this is in physical form, under lock and key. Our security measures and procedures reflect the seriousness with which we approach security and the value we attach to your information.

Only relevant members of staff will access the information you provide to us.

12. Storing your information and deleting it

Full House Theatre will enter the information into electronic databases which are stored securely with password access, in our company files located on SharePoint within Microsoft Office 365 cloud storage. [Click here for Microsoft's privacy policy.](#)

All information to be held securely for 7 years unless you instruct us to remove your data from our files. At the 7 year point, we follow the 'delete data procedure' to ensure destruction of data is thoroughly completed.

13. Your rights

In relation to the information which we hold about you, you are entitled to:

- Ask us for access to the information
- Ask us to rectify the information where it is inaccurate or is incomplete
- Ask us to erase the information and take steps to ask others who we have shared your information with to also erase it
- Ask us to limit what we do with your information
- Object to our use of your information and ask us to stop that use
- Instruct us to provide you with the information we hold about you in a structured and commonly used format or transmit that information directly to another organisation

Our obligations to comply with the above rights are subject to certain exemptions, e.g. retention of data for HMRC purposes. Where we are using your information with your consent, you are entitled to withdraw your consent at any time. The lawfulness of our use of your information before consent was withdrawn is not affected.

14. Visitors to our website under 13

The **Age Appropriate Design Code** developed in the UK restricts the age of consent to 13 for on-line services. Online, as defined by the **Information Society Services (ISS)** includes social media, messaging, news and education services, sales offering goods or services. If you are under the age of 13, you will need your parent or guardian's consent with Parental Responsibility before providing personal information to Full House Theatre which we may hold.

15. Holding / use of personal data for minors.

Under GDPR Article 8, the age of consent, i.e. when a child is required or able to give their consent for the processing of their own data, is **16**. Under this age, consent is required from an adult with **Parental Responsibility**.

A child with consent given by an adult with parental responsibility can withdraw their consent once they exceed the age of consent. If a child of age gives consent, a holder of PR can withdraw consent if they feel the child has not the capacity to fully understand the request for consent. (This also applies to a vulnerable adult who might not understand what they are giving consent for).

A child as a subject of research is able to request erasure as they get older and circumstances change. They must be aware if their data is still in use. Any request by a child of appropriate consent age (16) for erasure of data will be honoured.

You have the right to withdraw consent at any point.

Appendix Three

Full House Theatre Data Breach Policy

Introduction

Full House Theatre holds and processes personal data. This is a valuable asset that needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidental or deliberate) of any data breach that could compromise security.

Compromise of information, confidentiality, integrity may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

Purpose

Full House Theatre is obliged under the Data Protection Act (DPA) and General Data Protection Regulation (GDPR) to have in place mechanisms to ensure the security of all personal data. This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents.

Scope

This policy relates to all personal and sensitive data held by Full House Theatre regardless of format.

This policy applies to all Full House Theatre staff, including temporary, casual or agency staff and contractors, consultants, suppliers working for, or on behalf of Full House Theatre.

The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

Definition / Types of Breach

For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

An incident in the context of this policy is an event or action which may compromise the confidentiality or integrity of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to Full House Theatre information assets and/or reputation.

An incident includes but is not restricted to, the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- Human error

- ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it

Reporting an incident

Any individual who accesses, uses or manages Full House Theatre information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer (DPO) Harriet Hardie harriet@fullhouse.org.uk

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practical.

The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process. (*See below the form to be completed*).

All staff should be aware that any breach of the Data Protection Act may result in Full House Theatre’s Disciplinary Procedures being instigated.

Containment and Recovery

The DPO will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

The DPO will report the breach to the ICO within 72 hrs of the breach becoming known. *Guidance on when and how to notify ICO is available from their website at:*
https://ico.org.uk/media/1536/breach_reporting.pdf

An initial assessment will be made by the DPO in liaison with relevant staff to establish the severity of the breach.

The DPO will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The DPO will establish who may need to be notified as part of the initial containment and will inform the police, insurance company, etc. where appropriate (e.g. theft).

Advice from experts may be sought in resolving the incident promptly (e.g. IT support).

The DPO will determine the suitable course of action to be taken to ensure a resolution to the incident.

Investigation and Risk Assessment

An investigation will be undertaken by the DPO immediately and wherever possible within 24 hours of the breach being discovered / reported.

The DPO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:

- The type of data involved and its sensitivity
- The protections that are in place (e.g. encryptions)
- What's happened to the data, has it been lost or stolen?
- Whether the data could be put to any illegal or inappropriate use
- Who the individuals are, number of individuals involved and the potential effects on those data subject(s)
- Whether there are wider consequences to the breach

Notification

The DPO will determine who needs to be notified of the breach. Not every incident warrants full notification.

Every incident will be assessed on a case by case basis. The following will be considered:

- Whether there are any legal/contractual notification requirements;
- Whether notification would assist the individual affected – could they act on the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data?

Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact Full House Theatre for further information or to ask questions on what has occurred.

The DPO will consider if office staff should be informed regarding the breach and to be ready to handle any incoming enquiries (either from press or individuals).

All actions will be recorded by the DPO.

Evaluation and response

Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures
- Whether methods of transmission are secure; sharing minimum amount of data necessary
- Identifying weak points within existing security measures
- Staff awareness
- Implementing a data breach plan

If deemed necessary a report recommending any changes to systems, policies and procedures will be considered by the Full House Theatre Board of Trustees.

Section 1: Data Breach Report Form	
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
Received by the Data Protection Officer on (date)	
	Continue to Section 2

Section 2: Assessment of Severity	
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
<p>What is the nature of the information lost?</p> <p>Sensitive personal data (as defined in the Data Protection Act) relating to a living, identifiable individual's</p> <ul style="list-style-type: none"> a) Racial or ethnic origin; b) Political opinions or religious or philosophical beliefs; membership of a trade union; c) Physical or mental health or condition; d) Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas e) Personal information relating to vulnerable adults and children f) Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed. g) Spreadsheets of marks or grades obtained by participants, information about individual cases of discipline or sensitive negotiations which could adversely affect individuals. 	

<p>h) Security information that would compromise the safety of individuals if disclosed.</p>	
<p>How much data has been lost? If laptop lost/stolen: How recently was the laptop backed up onto central IT systems?</p>	
<p>Is the information unique? Will its loss have adverse operational, research, financial, legal, liability or reputational consequences for Full House?</p>	
<p>Data Protection Officer to consider whether the matter should be escalated.</p>	
	<p>Continue to Section 3</p>

Section 3: Action taken	To be completed by Data Protection Officer
Incident number	e.g. year/001
On (date):	
Action taken:	
Was incident reported to Police?	Yes/No If YES, notified on (date):
Follow up action required/recommended:	
Reported to Data Protection Officer on (date):	
Reported to other stakeholders (details, dates):	
For use of Data Protection Officer	
Notification to ICO	YES/NO If YES, notified on: Details:
Notification to data subjects	YES/NO If YES, notified on: Details:
Notification to other external, regulator/stakeholder	YES/NO If YES, notified on: Details: