Pattingham Drama Group - Data Policy

1. Introduction

Pattingham Drama Group (PDG) is committed to being transparent about how it collects and uses the personal data of its members and to meeting its data protection obligations. This policy sets out PDG's commitment to data protection, and individual rights and obligations in relation to personal data.

This policy applies to the personal data of members of PDG. Members of PDG are any individual who has completed the annual membership form and has been accepted as a member by the committee. Members also include individuals who have been granted life membership by PDG.

PDG has appointed its secretary as the person with responsibility for data protection compliance within PDG. He/she can be contacted at:

Secretary at Pattinghamdramagroup dot co dot uk (Please substitute appropriate symbol for 'at' and 'dot' and remove spaces.)

Questions about this policy, or requests for further information, should be directed to him/her.

Definitions

"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.

"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

2. Data protection principles

PDG processes personal data in accordance with the following data protection principles:

- personal data is processed lawfully, fairly and in a transparent manner.
- personal data is collected only for specified, explicit and legitimate purposes.
- personal data is processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- personal data is accurate and all reasonable steps are taken to ensure that inaccurate personal data is rectified or deleted without delay.
- personal data is kept only for the period necessary for processing.

- appropriate measures are adopted to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

PDG tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. Where PDG relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

PDG does not process special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law.

Members personal data is held in hard copy or electronic format, or both. The periods for which PDG holds personal data are contained in its privacy notices to individuals.

3. Individual rights

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

They can require the PDG 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 individual's interests override PDG's legitimate grounds for processing data (where the PDG relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful;
- 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 PDG's legitimate grounds for processing data; and
- make a subject access request.

To ask the PDG to take any of these steps, you should send the request to the Secretary's e-mail address as detailed in Paragraph 1 above.

4. Data security

PDG takes the security of personal data seriously. PDG has 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 PDG officers and authorised PDG members in the proper conduct of PDG business.

PDG does not engage third parties to process personal data on its behalf..

5. Data breaches

If PDG discovers that there has been a breach of a member's personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The PDG 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 tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

6. Individual responsibilities

Members are responsible for helping PDG keep their personal data up to date. Individuals should let PDG know if data provided to PDG changes, for example if an individual moves house or email address.

PDG officers and PDG authorised members may have access to the personal data of other members in the course of the proper conduct of PDG business Where this is the case, PDG relies on individuals to help meet its data protection obligations to all members

Individuals who have access to personal data are 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 PDG) 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 PDG'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 secretary immediately.

7. General

PDG reserves the right from time to time to amend this policy.