



King George V Fund for Actors & Actresses

Data Protection Policy

***Addressing the General Data Protection Regulation
(GDPR) 2018 [EU] and UK Data Protection Legislation***

For information on this Policy or to request Subject Access please contact the Secretary:

Email: mccuinj@shipleys.com

Telephone/Fax: 01708 743616

Post: The Secretary
King George V Fund for Actors & Actresses
C/o 21 Repton Gardens
Romford
RM2 5LS

Introduction

The King George V Fund for Actors & Actresses ('the Charity') holds personal data about its Trustees, Committee Members, Grantees, suppliers and other individuals for a variety of business purposes. This policy sets out how the Charity seeks to protect personal data and ensure that all those connected with the Charity understand the rules governing their use of personal data to which they have access in the course of their work.

Definitions

Business purposes

The purposes for which personal data may be used by the Charity:

Grant management, general administration and financial management of the Charity.

Business purposes include the following:

- *Compliance with our legal and governance obligations and good practice.*
- *Ensuring privacy policies are adhered to (such as policies covering email and internet use).*
- *Operational reasons, such as recording transactions, communication with Trustees, Committee Members and Grantees and payment of grants.*
- *Investigating complaints.*
- *Checking references, ensuring safe working practices, monitoring and managing access to administrative information.*

Personal data

Information relating to identifiable individuals, such as prospective, current and former Trustees, Committee Members, Grantees, self-employed officers, suppliers and other contacts.

Personal data may include: individuals' contact details, educational background, details of qualification certificates and diplomas, decorations held, education and skills, marital status and job title. The data will also include bank account details where this is required for the direct payment of grants.

Sensitive personal data

Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings is not requested, sought or held by the Charity. However, the Charity may specifically ask for details of physical or mental health of a prospective Grantee if the information is absolutely required to assess whether or not a Grant can and should be made with reference to our charitable charter.

Scope

This policy applies to all Trustees, Committee Members and Grantees of the Charity. This policy supplements any other policies relating to internet and email use. The Charity may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be communicated to all those concerned.

Who is responsible for this policy?

The Charity is not required to appoint a **Data Protection Officer**. The responsibility for this policy rests with the Trustees and is maintained and administered by the Secretary as the Data Processor.

Fair and lawful processing

The Charity must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that it should not process personal data unless the individual whose details it is processing has consented to it doing so.

The Data Processor's Responsibilities

- Keeping the Trustees and Committee Members updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and policies on a regular basis.
- Arranging data protection guidance and advice for all and those included in this policy when required.
- Answering questions on data protection from Trustees, Committee Members and Grantees if and when they arise.
- Responding to individuals who wish to know what data is being held on them by the Charity.
- Checking and approving with third parties that might handle the Charity's data any contracts or agreement regarding data processing.

Responsibilities of the Secretary

- Ensuring all systems, services, software and equipment meet acceptable security standards.
- Checking and scanning security hardware and software regularly to ensure it is functioning properly.
- Researching third-party services the Charity is considering using to store or process data.

The processing of all data must be:

- Necessary to deliver the Charity's services.
- In the Charity's legitimate interests and not unduly prejudice the individual's privacy.

In most cases this provision will apply to routine administration and grant making data processing activities.

The Charity has a Data Protection Privacy Notice which has been communicated to those concerned.

The notice:

- Sets out the purposes for which the Charity holds personal data.
- Highlights that the Charity does not engage in any marketing or fund raising activities and that personal information is never passed on to third parties without consent.
- Provides that individuals have a right of access to the personal data that is held about them

Accuracy and relevance

The Charity will ensure that any personal data it processes is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. It will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that inaccurate personal data relating to them is corrected. If an individual believes that information is inaccurate, he/she should record the fact that the accuracy of the information is disputed and inform the Secretary.

Personal data

Trustees, Committee Members and Grantees must take reasonable steps to ensure that personal data the Charity holds about them is accurate and updated as required. In the case of a change in personal circumstances, the Secretary should be informed so that the data can be updated in the records.

Data security

The Charity must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on its behalf, the Secretary will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
- Printed data should be shredded when it is no longer needed.
- Data stored on a computer should be protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used.
- It is not expected that any cloud service will be used to store data.
- Any servers containing personal data must be kept in a secure location, away from general office space.
- Data should be regularly backed up.
- Data should never be saved directly to mobile devices.
- All servers containing sensitive data must be approved and protected by security software and strong firewall systems.

Data retention

The Charity must not retain personal data for any longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained.

Subject access requests

Under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them. This requirement is included in the GDPR 2018 and is expected to be included in the UK Data Protection Act 2018 when it is enacted. Subject access requests from individuals should be referred immediately to the Secretary.

Individuals should contact the Secretary if they would like to request information that the Charity holds about them. There are also restrictions on the information to which they are entitled under applicable law.

Processing data in accordance with the individual's rights

The Charity will abide by any request from an individual not to use their personal data. The Charity will not communicate with an individual unless it has an existing business relationship with them.

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important to the Charity. The following are details on how we collect data and what we will do with it:

What information is being collected? – to include	Full Name, address, age, telephone and email contacts, professional experience, facial photo, bank account details where these are required to pay Grants.
Who is collecting it?	The Secretary, Trustees and Committee Members.
How is it collected?	Communication by post, email, telephone or personal conversation with the prospective Trustee, Committee Member or Grantee.
Why is it being collected?	To process appointment as Trustee or Committee Member and facilitate payment of Grants.
How will it be used?	To maintain the financial and administration records of the Charity; generate address labels, letters and emails and administer the payment of Grants.
Who will it be shared with?	Within the Charity: the Trustees, Committee Members and Grantees. Contact details are shared with the Trustees, Committee Members and with the Grantees as necessary.
Details of transfers to a foreign country and safeguards	No information is transferred to a foreign country.
Retention period	Names, contact details, appointment, resignation and death dates are maintained in the database as a historical record of the Charity's activities.

Conditions for processing

The Charity will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All those who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of the privacy notice.

Justification for personal data

The Charity will process personal data in compliance with all six data protection principles.

1 Consent

The data that the Charity collects is subject to active consent by the data subject. This consent can be revoked at any time.

2 Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done free of charge.

3 Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

4 Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Secretary will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

5 International data transfers

No data may be transferred outside of the EEA without first discussing it with the Secretary. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

6 Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All Trustees and Committee Members have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the Information Commissioner's Office (ICO) of any compliance failures that are material either in their own right or as part of a pattern of failures.

Monitoring

Everyone must observe this policy. The Secretary has overall responsibility for this policy. He will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply

The Charity takes compliance with this policy very seriously. Failure to comply puts Trustees, Committee Members and the Charity at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action or sanctions.

Any Trustee, Committee Member or Grantee with any questions or concerns about this policy should contact the Secretary.