MICHAEL CLARK COMPANY

Michael Clark Company
Data Protection Policy

Date: August 2015

Signed:

Review Date: August 2018

Introduction
Michael Clark Company needs to gather and use certain information about individuals. These can include business contacts, employees, trustees, dancers, audiences and other people the organisation has a relationship with or may need to contact. This policy describes how this personal and sensitive data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

This data protection policy ensures Michael Clark Company:

- Complies with data protection law and follows good practice
- Protects the rights of staff, trustees and other stakeholders
- Is open about how it stores and processes individual's data
- Protects itself from the risks of data breach

MCC is a not-for-profit organisation and is registered with the Information Commissioner's Office.

The Data Protection Act 1998 describes how organisations – including MCC – must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

There are eight principles of data processing with which the data controller must ensure compliance. In this instance, MCC is the 'Data Controller'.

Personal data shall be:

- Processed fairly and lawfully
- Obtained only for the purpose stated
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary for that purpose
- Processed in line with the rights of data subjects under the Act
- Secured by appropriate technical and organisational measures
- Not transferred to countries without adequate protection

This policy applies to Michael Clark Company; its staff, volunteers and other people working on behalf of Michael Clark Company.

It applies to all data the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names
- Addresses
- Contact information
- Passport details
- Plus any other information relating to individuals

This policy helps to protect Michael Clark Company from data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Everyone who works for or with Michael Clark Company has some responsibility for ensuring data is collected, stored and handled appropriately. All staff that handle personal data must ensure that it is processed in line with this policy and data protection principles.

Key areas of responsibility:

- The Board of Directors is ultimately responsible for ensuring that Michael Clark Company meets its legal obligations
- The General Manager, with the Associate Director, are responsible for:
  a) Keeping the Board updated about data protection responsibilities, risks and issues
  b) Reviewing all data protection procedures and related policies in line with an agreed schedule
  c) Arranging advice for the people covered by this policy
  d) Dealing with requests from individuals to see data MCC holds about them (also called Subject Access Requests)
  e) Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data
  f) Ensuring all systems, services and equipment used for storing data meet acceptable security standards
  g) Performing regular checks and scans to ensure security hardware and software is functioning properly
  h) Evaluating any third party services the company is considering using to store or process data. For instance cloud computing services
- The Communications Manager is responsible for:
  a) Approving any data protection statements attached to communications such as emails and letters
  b) Addressing any data protection queries from journalists or media outlets
  c) Where necessary working with other staff to ensure marketing initiatives abide by data protection principles

Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally, internally or externally.
- MCC will ensure the Data Protection Policy is available for all employees via the Staff Handbook.
- MCC will ensure staff managing and handling personal information are appropriately trained to do so and understands that they are directly and personally responsible for following good data protection practice

- Employees should keep all data secure by taking sensible precautions and following the guidelines
- In particular strong passwords must be used and they should never be shared
- Personal data should not be disclosed to unauthorised people, either internally or externally
- Data should be regularly reviewed and updated, if no longer required it should be deleted and disposed of confidentially
- Employees should request help from the General Manager, if they are unsure about any aspect of data protection

Data Storage
These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the General Manager.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer
- Data printouts should be shredded and disposed of securely when no longer required

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared with unauthorised staff
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service
- Servers containing personal data should be sited in a secure location
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's backup procedures
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones
- All servers and computers containing data should be protected by approved security software and a firewall

Data use
MCC will collect data for lawful purposes only, including but not limited to:

- Staff administration
- Fundraising
- Marketing
- Realising the objectives of the organisation

In the case of sensitive data, such as health, religion or gender, express consent must be obtained. Processing may be necessary to operate MCC policies, such as Health and Safety and Equal Opportunities.

In order for the organisation to carry out its activities some data may need to be shared with third parties, including outside the EEA. MCC will ensure that this is done only on a need to know basis and that transfer of information is done with adequate safeguards.

MCC will take appropriate technical and organisational security measures to safeguard personal information, such as:

- Ensuring individuals are made aware of the uses of the information collected and consent is obtained for any secondary uses of information or disclosures to third parties
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data Retention

MCC will retain personal information for as long and in such a way as to comply with good employment and data protection practice and legislation.

Currently all recruitment monitoring documentation is held for three years. For unsuccessful applicants this is from the date of application and for employees from the date their employment ceases. The data held will be for management and administrative use only, but MCC may from time to time need to disclose some data it holds to relevant third parties (e.g. where legally obliged to do so by HMRC or Arts Council England. For the purpose of information such as student loans or, where requested to do so by the staff member concerned, for the purpose of giving a reference).

MCC is legally obliged to keep financial records for a period of 7 years.

MCC will store historical emails for no more than 10 years. After this date they will be archived.

MCC will undertake assessment and deletion every year.

Some data may be given special consideration and retained for archival purposes. Consent for archive purposes must be obtained by MCC at the time of data collection by including this in the list of possible data uses. If permission was not obtained for this use, it should be sought at the time of archiving.

Data accuracy

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated.

- MCC will make it easy for data subjects to update the information MCC holds about them.
- Data should be updated as inaccuracies are discovered. For instance. If a contact can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the Communications Manager's responsibility to ensure marketing databases are kept updated and checked against industry suppression files every six months.

Subject access requests
All individuals who are the subject of personal data held by MCC 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.

If an individual contacts the company requesting this information this is called a subjected access request.

Subject access requests from individuals should be made by email, addressed to the General Manager (isabelle@michaelclarkcompany.com). The General Manager can supply a standard request form, although individuals do not have to use this. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Individuals may be subject to a charge of a maximum of £10 per subject access request. The data controller will aim to provide the relevant data within 30 days.

Disclosing data for other reasons
In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, MCC will disclose requested data. However, the General Manager will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Consequences of breaching the Act and this Policy
Staff will be informed that they can be criminally liable if they knowingly or recklessly disclose personal data in breach of the Act.

A serious breach of this policy will be a disciplinary offence. Such a breach will be dealt with under the MCC's disciplinary procedures as set out in our Staff Handbook. A serious breach would include a situation where a member of staff accesses another employee's personnel records without authority.