DATA PROTECTION MANUAL

Policy Owner: Data Manager
Last Updated: Aug 2015
Last Reviewed: July 2016
Next Review Date: July 2017
Version Number: v2.0

CONTENTS

FOREWORD

This Data Protection Manual is the means by which ICMP Management Ltd trading as the Institute of Contemporary Music Performance (the Institute) satisfies the requirements of its stakeholders with particular regard to management responsibility for Data Protection, Employee Data Protection, Management Information, Data Security and Freedom of Information.

The Institute is obliged to ensure that this Data Protection Manual is fully and completely understood by its employees, and that its procedures are implemented and maintained at all times. This Data Protection Manual has been produced in accordance with the requirements of the Data Protection Act 1998 (including EU Directive 95/46/EC). All of the components of the Data Protection system shall be periodically and systematically reviewed by both internal and external Quality Audit procedures.

The Institute's Data Manager is responsible for the control of all matters relating to the implementation of this Data Protection Manual; however, data protection compliance is fundamental to all the work undertaken by the Institute and, as such, all personnel at every level shall practise the procedures herein established.

DATA PROTECTION

POLICY

1.0 The Data Protection Act 1998 requires the Institute to maintain this Data Protection Policy, and to register as a Data Controller with the Information Commissioner's Office in order to guarantee compliance with the provisions of the Act.

1.1 Schedule 1 of the Data Protection Act 1998 sets out eight principles of Data Protection with which any party handling personal data must comply. To this end the Institute will ensure all personal data:

- shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Section 9.0 is met and, in the case of sensitive personal data, at least one of the conditions in Schedule 9.1 is also met (see *Conditions for Processing*, below)

- shall be obtained only for specified and lawful purposes and shall not be processed in any manner which is incompatible with those purposes
- shall be adequate, relevant and not excessive with respect to the purposes for which it is processed
- shall be accurate and, where appropriate, kept up-to-date;
- shall be kept for no longer than is necessary in light of the purpose(s) for which it is processed
- shall be processed in accordance with the rights of data subjects under the Act
- shall be protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures; and
- shall not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

PROCEDURE

Data Controller

2.0 The Institute's designated Data Controller is the Data Manager. He/She exercises the following responsibilities on behalf of the Board of Directors:

- ensuring that staff, students and authorised third parties comply with the data protection principles, as set out in legislation, in respect of personal data under their control
- ensuring that the Institute's Data Protection Manual is appropriate for the types of personal data being processed
- ensuring that the Institute maintains an up-to-date notification of its use of personal data with the Information Commissioner's Office

Data Protection Officer

3.0 The Institute's designated Data Protection Officer is also the Data Manager. He/she exercises the following responsibility on behalf of the Board of Directors:

- training and advising staff on the implementation of the Institute's Data Protection Manual
- monitoring compliance with the Institute's Data Protection, Employee Records Data Protection, Data Security and Freedom of Information policies.
- serving as the focal point for the administration of all subject access requests relating to personal data held by the Institute

Data Owner

4.0 A Data Owner is defined by the Act as a member of staff given authorised access to data which relates to a living individual who can be identified from that data or from that data as well as other information which is in the possession of, or is likely to come into the possession of, the data controller (including any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual).

4.1 Data Owners are responsible for:

- ensuring that the data is kept up-to-date and that amendments are made promptly following notification of changes
- ensuring that the security measures are appropriate for the types of personal data being processed

Responsibilities of Data Subjects

5.0 Data Subjects, whether staff, students or authorised third parties are responsible for:

- ensuring that any personal information that they provide to the Institute in connection with their employment, registration or other contractual agreement is accurate to the best of their knowledge
- informing the Institute of any changes to any personal information which they have provided, e.g. changes of address
- responding to requests to check the accuracy of the personal information held on them and processed by the Institute, details of which will be sent out from time to time, and informing the Institute of any errors that need amending

Notification to the Information Commissioner's Office

6.0 As a Data Controller, the Institute is required to notify the Information Commissioner's Office that it is processing personal data.

6.1 Data Controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify is a criminal offence.

6.2 Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place.

6.3 The Institute is registered in the register of data controllers with Registration Number: **Z2904555**.

6.4 The Data Manager shall be responsible for notifying and updating the Information Commissioner's Office.

Data Types

7.0 Personal data is defined by the Act as data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

7.1 The Act also defines “sensitive personal data” as personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious (or similar) beliefs; their physical or mental health condition; their sexual life; the commission or alleged commission by them of any offence; or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

7.2 The Institute only holds personal data which is directly relevant to its dealings with a given data subject.

7.3 The following data may be collected, held and processed by the Institute from time to time:

- Staff, Agent and Contractor Administration
  - Personal Details
  - Family, Lifestyle & Social Circumstances
  - Education & Training Details
  - Employment Details
  - Financial Details
  - Goods or Services Provided
  - Racial or Ethnic Origin
  - Trade Union Membership
  - Physical or Mental Health or Condition
  - Offences (Including Alleged Offences)

- Advertising, Marketing, Public Relations, General Advice Services
  - Personal Details
  - Family, Lifestyle & Social circumstances
  - Education & Training Details
  - Employment Details
  - Physical or Mental Health or Condition

- Accounts & Records
  - Personal Details
  - Employment Details
  - Financial Details
  - Goods or Services Provided

- Education
  - Personal details
  - Family, Lifestyle & Social Circumstances
  - Education & Training Details
  - Employment Details
  - Financial Details
  - Racial or Ethnic Origin
  - Religious or Other Beliefs of a Similar Nature
  - Physical or Mental Health or Condition
  - Offences (Including Alleged Offences)
  - Student Records

- Student & Staff Support Services
  - Personal details
  - Family, Lifestyle & Social Circumstances
  - Education & Training Details
  - Employment Details
  - Financial Details
  - Goods or Services Provided
  - Racial or Ethnic Origin
  - Religious or Other Beliefs of a Similar Nature
  - Trade Union Membership
  - Physical or Mental Health or Condition

- Crime Prevention and Prosecution of Offenders
    - Personal Details
    - Goods of Services Provided
    - Offences (Including Alleged Offences)
    - Criminal Proceedings, Outcomes & Sentences
    - Visual Image
    - Personal Appearance & Behaviour

- Data Controller's Free Text Description of Purpose
    - Personal Details
    - Goods or Services Provided
    - Photographic Images;
    - Text of Magazine Articles

Processing Personal Data

8.0 All personal data held by the Institute is collected in order to ensure that the Institute can facilitate efficient transactions with third parties including, but not limited to, its customers, partners, associates and affiliates and efficiently manage its employees, contractors, agents and consultants. Personal data shall also be used by the Institute in meeting any and all relevant obligations imposed by law.

8.1 Personal data may be disclosed within the Institute. Personal data may be passed from one department to another in accordance with the data protection principles. Under no circumstances will personal data be passed to any department or any individual within the Institute that does not reasonably require access to that personal data with respect to the purpose(s) for which it was collected and is being processed.

8.1.2 The Institute shall ensure that:

- all personal data collected and processed for and on behalf of the Institute by any party is collected and processed fairly and lawfully
- data subjects are made fully aware of the reasons for the collection of personal data and are given details of the purpose for which the data will be used
- personal data is only collected to the extent that is necessary to fulfil the stated purpose(s)
- data subjects are informed of their responsibility to ensure that their personal data is accurate at the time of collection and kept accurate and up-to-date while it is being held and / or processed

- personal data is held for no longer than necessary in light of the stated purpose(s)
- personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect the data
- personal data is transferred using secure means, electronically or otherwise
- personal data is not transferred outside of the UK or EEA (as appropriate) without first ensuring that appropriate safeguards are in place in the destination country or territory
- data subjects can exercise their rights as detailed below and set out more fully in the Act

Conditions for Processing

9.0 At least one of the following conditions must be met whenever the Institute processes personal data:

- the individual to whom the personal data refers has consented to the processing.
- the processing is necessary in relation to a contract which the individual has entered into or because the individual has asked for something to be done so they can enter into a contract.
- the processing is necessary because of a statutory obligation that applies to an individual
- the processing is necessary to protect the individual's "vital interests"; this condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident
- the processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
- the processing is in accordance with the "legitimate interests" condition

9.1 In addition to the conditions described in Section 8.0 above, at least one of the following conditions must also be met whenever the Institute processes sensitive personal data (as described in Section 7.1 above):

- the individual who the sensitive personal refers to has given explicit consent to the processing
- the processing is necessary to comply with employment law
- the processing is necessary to protect the vital interests of the individual (in a case where the individual's consent cannot be given or reasonably obtained) or another person (in a case where the individual's consent has been unreasonably withheld)
- the processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents
- the individual has deliberately made the information public
- the processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights
- the processing is necessary for administering justice, or for exercising statutory or governmental functions
- the processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality

- the processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals

Organisational Measures

10.0 The Institute shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

- a Data Protection Officer will be appointed with the specific responsibility of overseeing data protection and ensuring compliance with the Act
- all employees, contractors, agents, consultants, partners or other parties working on behalf of the Institute will be furnished with a copy of this Data Protection Manual
- all employees, contractors, agents, consultants, partners or other parties working on behalf of the Institute will be made fully aware of both their individual responsibilities and the Institute's responsibilities under the Act
- all employees, contractors, agents, consultants, partners or other parties working on behalf of the Institute handling personal data will be appropriately trained to do so
- all employees, contractors, agents, consultants, partners or other parties working on behalf of the Institute handling personal data will be appropriately supervised
- methods of collecting, holding and processing personal data will be regularly evaluated and reviewed
- the performance of those employees, contractors, agents, consultants, partners or other parties working on behalf of the Institute handling personal data will be regularly evaluated and reviewed
- all employees, contractors, agents, consultants, partners or other parties working on behalf of the Institute handling personal data will be bound to do so in accordance with the principles of the Act and this Data Protection Manual by contract; failure by any employee to comply with the principles or this Data Protection Manual shall constitute a disciplinary offence; failure by any contractor, agent, consultant, partner or other party to comply with the principles or this Data Protection Manual shall constitute a breach of contract; in all cases, failure to comply with the principles or this Data Protection Manual may also constitute a criminal offence under the Act
- all contractors, agents, consultants, partners or other parties working on behalf of the Institute handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Institute arising out of this Data Protection Manual and the Act
- where any contractor, agent, consultant, partner or other party working on behalf of the Institute handling personal data fails in their obligations under this Data Protection Manual that party shall indemnify and hold harmless the Institute against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure

Rights of Data Subjects

10.1 Under the Act, Data Subjects have:

- the right to be informed that their personal data is being processed
- the right to access any of their personal data held by the Institute within 40 calendar days of making a request
- the right to prevent the processing of their personal data in limited circumstances
- the right to rectify, block, erase or destroy incorrect personal data

Access by Data Subjects

11.0 A Data Subject may make a subject access request ("SAR") at any time to see the information which the Institute holds about them>

11.1 SARs must be made in writing, accompanied by the correct fee; the Institute currently requires a fee of £10.00 (the statutory maximum) for all SARs excluding credit file requests (which attract a fee of £2.00).

11.2 Upon receipt of a SAR the Institute shall have a maximum period of 40 working days within which to respond. The following information will be provided to the data subject:

- whether or not the Institute holds any personal data on the data subject
- a description of any personal data held on the data subject
- details of what that personal data is used for
- details of any third-party organisations that personal data is passed to
- details of any technical terminology or codes

EMPLOYEE RECORDS DATA PROTECTION

POLICY

1.0 The Institute collects employee related personal data in order to ensure that the Institute can effectively manage and facilitate efficient transactions with its employees and contractors as well as to comply with relevant employment law. The Human Resources Manager is the primary handler and administrator of all subject access requests relating to personnel data held by the Institute.

1.1 The Employee Records Data Protection Policy does not form part of the formal contract of employment and/or service provision, but it is a condition of engagement that all employees/contractors will abide by it at all times.

PROCEDURE

Monitoring

2.0 The Institute may from time to time monitor the activities of employees; such monitoring may include, but will not necessarily be limited to, internet and email monitoring.

2.1 Any employee that is to be monitored shall be informed in advance of such monitoring; however, under no circumstances will monitoring interfere with an employee's normal duties.

2.2 The Institute shall use its best and reasonable endeavours to ensure that there is no intrusion upon employees' personal communications or activities and under no circumstances will monitoring take place outside of the employee's normal place of work or work hours.

Benefits

3.0 In cases where employees are enrolled in benefit schemes that are provided by the Institute (including, but not limited to, pensions and healthcare) it may be necessary from time to time for third party organisations to collect personal data from relevant employees. Prior to collection, employees will be fully informed of the personal data that is to be collected, the reasons for its collection, and the way(s) in which it will be processed. The Institute shall not use any such data except insofar as is necessary in the administration of relevant benefits schemes.

Health Records

4.0 The Institute holds health records on all employees in order to assess the health, wellbeing and welfare of employees and highlight any issues which may require further investigation. Such health records include details of sick leave, medical conditions, disabilities and prescribed medication. Data under this heading will be used by management only and will not be revealed to fellow employees and peers (unless those employees are responsible for health records in the normal course of their duties).

4.1 Employees have the right to request that the Institute does not keep health records on them. All such requests must be made in writing and addressed to the Human Resources Manager.

Employee Records and Retention

5.0 Personal data processed for any purpose shall not be kept for longer than is necessary for those purposes (normally six years following the cessation of the working relationship) or as required to comply with legislation.

DATA SECURITY

POLICY

1.0 The Institute collectively, and its staff and students individually, are responsible for ensuring that appropriate technical and organisational measures are taken against the unauthorised or unlawful processing of personal data as well as against accidental loss or destruction of, or damage to, personal data.

PROCEDURE

1.1 Institute staff and students must ensure that they employ safeguards for personal data that is proportional to the risks presented in their processing activities.

1.2 Any staff or students who discover a potential or actual security breach must immediately inform the Data Manager.

1.3 The Institute will ensure that all of its employees, contractors, agents, consultants, partners or other parties working on behalf of the Institute comply with the following when processing and / or transmitting personal data:

- all emails containing personal data will be encrypted
- personal data may only be transmitted over secure networks; transmission over unsecured networks is not permitted under any circumstances
- personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable
- personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely; the email itself, and any temporary files associated therewith, should be deleted
- where personal data is to be sent by facsimile transmission, the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data
- where personal data is to be transferred in hardcopy form it should be passed directly to the recipient; the use of an intermediary is not permitted
- all hardcopies of personal data should be stored securely in a locked box, drawer, cabinet or similar

- all electronic copies of personal data should be stored securely using passwords and suitable data encryption, where possible on a drive or server which cannot be accessed via the internet; the use of portable storage devices is not permitted

- all passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised

FREEDOM OF INFORMATION

POLICY

1.0 The Freedom of Information Act 2000 imposes upon all public sector institutions an obligation to provide the public with wide rights of access to their records and guarantees the public a statutory right to:

- obtain (either from the Institute's website or in some other form) all the information covered by the organisation's Publication Scheme
- request (within the limitations outlined in the Data Protection Act 1998) any information held by the organisation, regardless of when it was created, by whom, or the form in which it is now recorded

1.1 As a private sector institution with quasi-public sector functions, the Institute is not bound by the Freedom of Information Act 2000; however, the Institute is committed to being open and honest in the conduct of its operations. To this end, the Institute will:

- be open with the general public and the media and will place in the public domain as much information about its activities as is practicable