The Institute of Contemporary Music Performance

Data Protection Policy

Version number	Date approved (including committee)	Reason for production/revision	Author	Proposed next review date
V1.0	Sept 2021 ExCo	Replacing the DP manual, this is aligned with the Information Governance Framework	Business Development Director	Biennially and as required

Related policies
Freedom of Information Policy Employee Records Data Protection Policy Records Management Policy Data Security Policy Email Use Policy Acceptable Us of IT Policy Bring Your Own Device Policy Business Continuity Policy Staff Disciplinary Policy Student Disciplinary Policy Equality & Diversity Policy Safeguarding Policy
External Reference
General Data Protection Regulation (GDPR), UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulation (PECR), Freedom of Information Act 2000, Environmental Information Regulations 2004

ICMP

The Institute
of Contemporary
Music Performance

1. INTRODUCTION

1.1. This Data Protection Policy is the means by which ICMP Management Ltd trading as the Institute of Contemporary Music Performance (ICMP) satisfies the requirements of its stakeholders with particular regard to management responsibility for Data Protection.

1.2. ICMP is obliged to ensure that this Data Protection Policy and the suite of Information Governance Policies that compliment it are fully and completely understood by its employees, and that its procedures are implemented and maintained at all times. This Data Protection Policy has been produced in accordance with ICMP's obligations under the Data Protection Legislation (this includes the General Data Protection Regulation (the GDPR), the UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulation (PECR)). All components of the Data Protection system shall be periodically and systematically reviewed by both internal and external Quality Audit procedures.

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

2. POLICY

2.1. The Data Protection Act 2018 requires ICMP 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.

2.2. Schedule 1 of the Data Protection Act 2018 sets out eight principles of Data Protection with which any party handling personal data must comply. To this end ICMP will ensure all personal data:

2.2.1. shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Article 6 of the GDPR is met (see *Conditions for Processing*, below)

2.2.2. shall be obtained only for specified and lawful purposes and shall not be processed in any manner which is incompatible with those purposes

2.2.3. shall be adequate, relevant and not excessive with respect to the purposes for which it is processed

2.2.4. shall be accurate and, where appropriate, kept up-to-date;

2.2.5. shall be kept for no longer than is necessary in light of the purpose(s) for which it is processed

2.2.6. shall be processed in accordance with the rights of data subjects under the Act

2.2.7. shall be protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures; and

2.2.8. 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.

3. PROCEDURE

Data Controller.

3.1. ICMP is the Data Controller for our data processing – we determine the purposes and means of processing personal data. We will usually also be the data processor responsible for the actual processing of personal data.

3.2. Where we use another organisation as data processor (for instance an IT service provider), we remain responsible for ensuring that data processing is carried out in line with the GDPR.

3.3. In certain cases (for instance where we collaborate with our awarding bodies, or where the Higher Education Statistics Agency collects data from us) both we and

another agency may be Data Controllers in relation to the processing of the same data. We are not the Data Processor for HESA or any other regulatory body.

Data Protection Officer

3.4. ICMP's designated Data Protection Officer (DPO) is the Business Development Director. They exercise the following responsibility on behalf of the Board of Directors:

3.4.1. training and advising staff on the implementation of ICMP's Data Protection Policy and suite of Information Governance Policies

3.4.2. monitoring compliance with ICMP's Data Protection, Employee Records Data Protection, Data Security and Freedom of Information policies.

3.4.3. serving as the focal point for the administration of all subject access requests relating to personal data held by the Institute.

Staff

3.5. Each member of staff with access to personal data is responsible for:

3.5.1. ensuring that the data is kept up-to-date and that amendments are made promptly following notification of changes.

3.5.2. ensuring that the security measures are appropriate for the types of personal data being processed.

Responsibilities of Data Subjects

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

3.6.1. ensuring that any personal information that they provide to ICMP in connection with their employment, registration or other contractual agreement is accurate to the best of their knowledge

3.6.2. informing ICMP of any changes to any personal information which they have provided, e.g. changes of address

3.6.3. responding to requests to check the accuracy of the personal information held on them and processed by ICMP, details of which will be sent out from time to time, and informing ICMP of any errors that need amending

Notification to the Information Commissioner's Office

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

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

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

3.10. ICMP is registered in the register of data controllers with Registration Number: **Z2904555**.

3.11. The DPO shall be responsible for notifying and updating the Information Commissioner's Office.

Data Types

3.12. Personal data is data which relates to a living individual 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.

3.13. The GDPR also defines "special category data". Special category data is more sensitive, and so needs more protection. For example, information about an individual's:

3.13.1. race;

3.13.2. ethnic origin;

3.13.3. politics;

3.13.4. religion;

3.13.5. trade union membership;

3.13.6. genetics;

3.13.7. biometrics (where used for ID purposes);

3.13.8. health;

3.13.9. sex life; or

3.13.10. sexual orientation.

3.14. ICMP only holds personal data which is directly relevant to its dealings with a given data subject.

3.15. The following data may be collected, held and processed by ICMP from time to time:

3.16. **Staff, Agent and Contractor Administration**

3.16.1. Personal Details

3.16.2. Family, Lifestyle & Social Circumstances

3.16.3. Education & Training Details

3.16.4. Employment Details

3.16.5. Financial Details

3.16.6. Goods or Services Provided

3.16.7. Racial or Ethnic Origin

3.16.8. Trade Union Membership

3.16.9. Physical or Mental Health or Condition

3.16.10. Offences (Including Alleged Offences)

3.17. **Advertising, Marketing, Public Relations, General Advice Services**

3.17.1. Personal Details

3.17.2. Family, Lifestyle & Social circumstances

3.17.3. Education & Training Details

3.17.4. Employment Details

3.17.5. Physical or Mental Health or Condition

3.18. **Accounts & Records**

3.18.1. Personal Details

3.18.2. Employment Details

3.18.3. Financial Details

3.18.4. Goods or Services Provided

3.19. **Education**

3.19.1. Personal details

3.19.2. Family, Lifestyle & Social Circumstances

3.19.3. Education & Training Details

3.19.4. Employment Details

3.19.5. Financial Details

3.19.6. Racial or Ethnic Origin

3.19.7. Religious or Other Beliefs of a Similar Nature

3.19.8. Physical or Mental Health or Condition

3.19.9. Offences (Including Alleged Offences)

3.19.10. Student Records

3.20. **Student & Staff Support Services**

3.20.1. Personal details

3.20.2. Family, Lifestyle & Social Circumstances

3.20.3. Education & Training Details

3.20.4. Employment Details

3.20.5. Financial Details

3.20.6. Goods or Services Provided

3.20.7. Racial or Ethnic Origin

3.20.8. Religious or Other Beliefs of a Similar Nature

3.20.9. Trade Union Membership

3.20.10. Physical or Mental Health or Condition

3.21. **Crime Prevention and Prosecution of Offenders**

3.21.1. Personal Details

3.21.2. Goods of Services Provided

3.21.3. Offences (Including Alleged Offences)

3.21.4. Criminal Proceedings, Outcomes & Sentences

3.21.5. Visual Image

3.21.6. Personal Appearance & Behaviour

Processing Personal Data

3.22. All personal data held by ICMP is collected in order to ensure that ICMP 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 ICMP in meeting any and all relevant obligations imposed by law.

3.23. Personal data may be disclosed within ICMP. 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 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. Data subjects

may authorise nominated third parties to have access to personal data by emailing or writing to ICMP.

3.24. ICMP shall ensure that:

3.24.1. all personal data collected and processed for and on behalf of ICMP by any party is collected and processed fairly and lawfully

3.24.2. 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

3.24.3. personal data is only collected to the extent that is necessary to fulfil the stated purpose(s)

3.24.4. 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

3.24.5. personal data is held for no longer than necessary in light of the stated purpose(s)

3.24.6. personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect the data

3.24.7. personal data is transferred using secure means, electronically or otherwise

3.24.8. 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

3.24.9. data subjects can exercise their rights as detailed below and set out more fully in the GDPR

Lawful Basis for Processing

3.25. The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever ICMP processes personal data:

(a) Consent: the individual has given clear consent to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract with the individual, or because they have asked ICMP to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for ICMP to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for ICMP to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

3.26. The lawful basis for some data processing at ICMP will be to fulfil a contract, for example with our staff. ICMP is registered as an HEI under the Approved (fee cap) category with the Office for Students (OfS). As such, ICMP is considered a 'Public Authority' as described within Schedule 1 of the Freedom of Information Act 2020. As a 'Public Authority' ICMP considers the lawful basis for processing most student data as being 'public good'

3.27. The basis for specific processing will be contained within the corresponding privacy statement.

3.28. In order to lawfully process special category data, ICMP must identify both a lawful basis under Article 6 of GDPR and a separate condition for processing special category data under Article 9. The conditions are:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Organisational Measures

3.29. ICMP shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

3.29.1. a Data Protection Officer will be appointed with the specific responsibility of overseeing data protection and ensuring compliance with the GDPR

3.29.2. all employees, contractors, agents, consultants, partners or other parties processing data on behalf of ICMP will be furnished with a copy of this Data Protection Policy

3.29.3. all employees, contractors, agents, consultants, partners or other parties processing data on behalf of ICMP will be made fully aware of both their individual responsibilities and ICMP's responsibilities under the GDPR and the 2018 Act

3.29.4. all employees, contractors, agents, consultants, partners or other parties working on behalf of ICMP handling personal data will be appropriately trained to do so

3.29.5. all employees, contractors, agents, consultants, partners or other parties working on behalf of ICMP handling personal data will be appropriately supervised

3.29.6. methods of collecting, holding and processing personal data will be regularly evaluated and reviewed

3.29.7. the performance of those employees, contractors, agents, consultants, partners or other parties working on behalf of ICMP handling personal data will be regularly evaluated and reviewed

3.29.8. all employees, contractors, agents, consultants, partners or other parties working on behalf of ICMP handling personal data will be bound to do so in accordance with the principles of the GDPR, 2018 Act and this Data Protection Manual by contract; failure by any employee to comply with the principles or this Data Protection Policy shall constitute a disciplinary offence; failure by any contractor, agent, consultant, partner or other party to comply with the principles or this Data Protection Policy shall constitute a breach of contract; in all cases, failure to comply with the principles or this Data Protection Policy may also constitute a criminal offence under the Act

3.29.9. all contractors, agents, consultants, partners or other parties working on behalf of ICMP 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 ICMP arising out of this Data Protection Policy and the Act

3.29.10. where any contractor, agent, consultant, partner or other party working on behalf of ICMP handling personal data fails in their obligations under this Data Protection Policy that party shall indemnify and hold harmless ICMP against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure

Rights of Data Subjects

3.30. Under the GDPR, Data Subjects have:

3.30.1. The right to be informed

3.30.2. The right of access

3.30.3. The right to rectification

3.30.4. The right to erasure

3.30.5. The right to restrict processing

3.30.6. The right to data portability

3.30.7. The right to object

3.30.8. Rights in relation to automated decision making and profiling.

Access by Data Subjects

3.31. Individual data subjects have the right to obtain the following from ICMP:

3.31.1. confirmation that we are processing their personal data;

3.31.2. a copy of their personal data; and

3.31.3. other supplementary information.

3.32. This is sometimes referred to as a 'Subject Access Request' (SAR).

3.33. The GDPR does not specify how to make a valid request. Therefore, an individual can make a subject access request to us verbally or in writing. It can also be made to any part of ICMP (including by social media) and does not have to be to a specific person or contact point. There is no special form of words that must be used

3.34. Upon receipt of a SAR, ICMP shall have a maximum period of one month within which to respond. The following information will be provided to the data subject:

3.34.1. whether or not ICMP holds any personal data on the data subject

3.34.2. a copy of any personal data held on the data subject

3.34.3. details of what that personal data is used for

3.34.4. details of any third-party organisations that personal data is passed to

3.34.5. details of any technical terminology or codes

3.35. Where a SAR is very broad (for instance asking for all data held by ICMP about a student), it is permissible for ICMP to seek clarification about the data actually requested in order to avoid confusion to the data subject when they receive the data.

Right to be Forgotten

3.36. Under the GDPR, data subjects have a 'right to be forgotten'. On request, ICMP will destroy data relating to that data subject.

3.37. Individuals have the right to have their personal data erased if:

3.37.1. the personal data are no longer necessary for the purpose which we originally collected or processed it for;

3.37.2. we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;

3.37.3. we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;

3.37.4. we are processing the personal data for direct marketing purposes and the individual objects to that processing;

3.37.5. we have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);

3.37.6. we have to do it to comply with a legal obligation; or

3.37.7. we have processed the personal data to offer information society services to a child.

3.38. This means that we will not erase data that have been returned to HESA, OfS, UKVI or HMRC (or form part of the audit trail for such data), or other data for which we have a continuing legitimate need (for instance records about a data subject who owes us money). We may also refuse to comply with a request for erasure if it is manifestly unfounded or excessive, asking into account whether the request is repetitive in nature.

3.39. The GDPR does not specify how to make a valid request. Therefore, an individual can make a request for erasure verbally or in writing. It can also be made to any part of our organisation and does not have to be to a specific person or contact point. A request does not have to include the phrase 'request for erasure' or Article 17 of the GDPR. No fee is charged.

On receipt of a request we will consider whether we are obliged to erase data and erase any data for which the conditions in section 12.1 are met. We will ensure that data are also deleted from backup systems. We have one calendar month to comply.