APPENDIX

Data Protection Policy

1) Introduction

The CMI needs to keep certain personal data and sensitive personal data, for example about staff, customers, guests and donors, in order to fulfil its purpose.

Under the provisions of the Data Protection Act 1998, which came into force on 1 March 2000 and the General Data Protection Regulation 2018, the organisation has a legal duty to ensure that personal information is collected and used fairly, stored safely and not disclosed to any other person or organisation unlawfully. The purpose of the Act is 'to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy' and in doing so it also provides data subjects (ie. individuals about whom personal information/sensitive personal information is processed) increased protection through express new rights.

The General Data Protection Regulation (GDPR) gives individual even more rights and requires organisations to be more transparent about their activities in regards to personal data, therefore CMI will review and update all processes and procedures to reflect required compliance.

2) Scope

The aim of this policy is both to ensure that all staff are aware of their particular responsibilities in relation to the Data Protection Act and its associated codes of practices; and to inform members of the public how CMI complies with the legislation. Its other purpose. is to minimise the risk of the CMI breaching the Act; thereby potentially damaging valued relationships with staff and customers as well as its reputation and potentially incurring financial fines.

This policy covers all **personal data** and **sensitive personal data** held in **electronic** format or in **relevant manual filing systems** that is **processed** by the CMI. (For definitions see below).

It applies to all individuals working for the CMI in whatever role. This includes permanent and contracted staff, as well as temporary employees; volunteers; interns etc.

The security of information held by CMI is governed by the organisation's Information Security Policy.

3) Definitions

Under the terms of the Act:

- **Personal data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, visual, physiological, genetic, mental, economic, cultural or social identity of that natural person. This excludes business or commercial engagement.
- **Sensitive personal data** is a subset of personal data and subject to tighter controls on its processing. Sensitive personal data means personal data consisting of information as to -
    - the racial or ethnic origin of the data subject,
    - his / her political opinions,
    - his / her religious beliefs or other beliefs of a similar nature,
    - whether he / she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
    - his / her physical or mental health or condition,
    - his / her sexual life,
    - the commission or alleged commission by him / her of any offence, or
    - any proceedings for any offence committed or alleged to have been committed by him / her, the disposal of such proceedings or the sentence of any court in such proceedings.

- **Data subject** means the individual about whom the personal data/sensitive personal data is held.
- **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **Electronic format** means data held as word or excel documents, e-mails, in databases, payroll systems, the Festival Management system (FMP) etc.
- Relevant **manual filing systems** means a filing system in which information about individuals is readily available. For example, files ordered alphabetically by name (staff files, member files, notes on guests) or by which there is another point of access (reference number system etc.). It does not apply to incidental references to individuals in files structured by reference to topics not relating to those individuals.

4) Legal Basis

The CMI's responsibilities in relation to data protection are determined by the General Data Protection Regulation (2018) and the Data Protection Act (1998).

5) Statement of Principles

The CMI is accountable and is therefore committed to the **Data Protection Principles** contained in the Data Protection Act 1998 and updated by the General Data Protection Regulation 2018. These represent the minimum standards of practice for any organisation with respect to personal data/sensitive personal data and state that it must be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject
2. collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
3. **adequate, relevant and limited** to what is necessary in relation to the purposes for which they are processed accurate and kept up to date
4. **accurate and, where necessary, kept up to date;** every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
5. **kept in a form which permits identification of data subjects** for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to **implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject**
6. processed in a manner that ensures appropriate **security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Going forward the CMI will comply with the General Data Protection Regulation (2018) requirements by reviewing and creating additional internal process for secure storing, processing and disposing of personal data and sensitive personal data.

6) Rights of Data Subjects

- Any individual data subject, including staff, guests and members, have the right to ask what information the CMI holds about them and why this is being held.

- If any such information is held, an individual data subject also has the right, on request:
    - to see any personal data/sensitive personal data that is being kept about them on computer, and also to have access to paper based data held in relevant manual filing systems
    - to be informed as to how to get the information updated or amended

- to be informed as to any regular or possible recipients of the information.

- Any person who wishes to exercise this right should make the request in writing to the Office Administrator. If an access request is received by any other members of staff it should be forwarded to the Office Administrator. Alternatively if an access request is related to an existing or ex-member of staff / volunteer it should be forwarded to the HR department (currently Gravitate).

- The CMI will comply with requests for access to personal information as quickly as possible. In compliance with the law, this will always be within 40 calendar days of receipt of a request. From May 2018 this will be processed with one calendar month. This service is free of charge.

- As well as right of subject access, individual data subjects have the right to object to direct marketing, including marketing of the CMI's products and services. Where an individual decides to exercise this right, this fact should be accurately recorded.

- As well as a right of subject access, individual data subjects may, in certain circumstances, have other rights under the Act, including the right to have inaccurate information corrected. The Office Administrator should be informed if a request to exercise this right is received.

7) Responsibilities

- The **Board of Trustees** of the CMI is the **Data Controller.** The Data Controller is the legal entity who must comply with the Act and the Regulation and ensure that its provisions are upheld in all processing across the organisation.

- The Chief Operating Officer acts as CMI's **Data Protection Officer.** The Data Protection Officer is accountable and responsible for overseeing all Data Protection activities and promoting compliance throughout the CMI. Under the terms of the Act, the organisation is obliged to prepare an annual notification to the Information Commissioner providing details of the types of data it processes and for what purpose. The Data Protection Officer is the individual responsible for ensuring that the CMI's entry is complete and up-to-date with assistance from relevant Heads of Department. The Data Protection Officer will ensure the CMI Board are able to review the entry annually before submission. The current register entry can be found through the Information Commissioner's website.

- The **HR Department** (Gravitate) will ensure that appropriate guidance and training on compliance with the Data Protection Act 1998 and General Data Protection Regulation 2018 is made available to all staff engaged in the processing of personal data/sensitive personal data.

- **The Chief Operating Officer** is responsible for determining retention periods for records. The Office Administrator acts as the first point of contact for data protection queries throughout the CMI, makes suggestions for best practice and identifies areas of risk. The Office Administrator works with staff who process personal data/sensitive personal data and Heads of Department to promote compliance within departments but it is the responsibility of Heads of Department to address any risks identified and to ensure that the provisions of the Act are upheld (see below).

- **Heads of Departments** are accountable for data protection compliance in their departments. It is their responsibility to ensure that all processing within their area complies with the Act, in particular that all points of personal data/sensitive personal data collection include appropriate data protection statements and that any contracts or agreements with external contractors processing personal data/sensitive personal data on the CMI's behalf (e.g. distribution or mailing services, data convertors etc.) include a relevant data protection clause. Heads of Department are responsible for ensuring that risks are identified and managed appropriately, that staff receive adequate training and that legal advice is sought where necessary.

- **Staff who process personal data/sensitive personal data in the course of their work** are responsible for ensuring compliance with the legislation and this policy document in their area. It is their responsibility to be aware of the terms of the Act and to raise any concerns about how personal data/sensitive personal data is collected and managed in their area with their Head of Department. The CMI will ensure they are given appropriate training to fulfil this responsibility. Staff must also advise the Data Protection Officer of any changes to data processing in their areas, so that the organisation's Register of Records caught by the Act can be amended accordingly.

- **All external data processors** processing personal data/sensitive personal data on behalf of the CMI (i.e. third parties) are contractually required to comply with the Data Protection Act 1998 and GDPR and any associated codes of practice. Heads of Department are responsible for ensuring that this is upheld (see above).

8) Procedures

The CMI will organise an annual training session for all staff. Additional best practice procedures will be available on the internal staff network drive.

9) Breach

Breach of data protection legislation is a criminal and potentially civil offence and the CMI will regard wilful or reckless breach of this policy as a disciplinary offence and such breaches will be subject to the CMI's disciplinary procedures.

It is the duty of all members of staff to flag immediately to their Head of Department and the Data Protection Officer any matter arising which involves, or is thought to

involve, a breach of data protection legislation. Any serious breach will be reported to the Chair of the Audit and Risk Committee.

Breach of data occurring in the CMI will be reported to those whose data might have been affected by the breach, as well as the supervisory authority within 72 hours of the breach occurring.

10) Review

This policy will be reviewed annually.
Next review: March 2019

11) Date of Approval

Approved at the CMI Board meeting on 13 March 2018.