MIoD Data Protection and Retention Policy

1. **Background**

1.1. MIoD needs to keep certain information about its employees and members to allow it to manage its membership, business and monitor performance. It is also necessary to process information so that the MIoD can comply with its legal obligations and so that employees can be recruited and members pay their dues and attend MIoD events and workshops. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

1.2. The Data Protection Act 2004 (the 'Act') places an obligation upon the MIoD, as a data controller, to collect and use personal data in a responsible and accountable manner. The MIoD is committed to ensuring that every current employee and registered member complies with this Act to ensure the confidentiality of any personal data held by the MIoD in whatever medium. Two key concepts to be considered are those of purpose and transparency.

1.3. Words used in this policy have the same definition as set out in the Act. For ease of use, the key terms used in the policy have been defined in the Glossary in Annex 1 to the policy.

2. **Basic principles**

2.1. The basic principles which apply are that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to any other third party without the data subject's authorisation.

3. **Compliance**

3.1. The MIoD and all its employees or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the MIoD has developed this Data Protection and Retention Policy.

4. **Status of the policy**

4.1. This policy does not form part of the formal contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the MIoD from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

5. **Data Controller**

5.1. The MIoD is the Data Controller as specified by the Act, and the Board is therefore ultimately responsible for implementation. The Board has designated three Data Controllers namely the CEO, the Executive Secretary and the Accounts and Administration Coordinator**,** to deal with day-to-day matters.

5.2. Any employee or member who considers that this Policy has not been followed in respect of personal data about himself or herself should raise the matter with the appropriate Designated Data Controller, who would be:

- For employees: the CEO
- For members: the Executive Secretary and the Accounts and Administration Coordinator.

6. **Responsibility**

6.1. All employees and members are responsible for:

- Checking that any information that they provide to the MIoD in connection with their employment and membership is accurate and up to date.
- Informing the MIoD of any changes to information that they have provided, e.g. changes of address, either at the time of appointment or subsequently. The MIoD cannot be held responsible for any errors unless the employee or member has informed the MIoD of such changes.

6.2. If and when, as part of their responsibilities, employees collect information about other people (e.g. members, other employees), they must comply with the guidelines for employees set out in this Policy.

6.3. Employees can only process personal data where they have a clear purpose for doing so, and then only as necessitated by that purpose. Paragraph 17 of this Code of Practice summarises the main purposes for which the MIoD processes personal data.

7. **Collection of personal data**

7.1. In most cases, the personal data held by the MIoD will be obtained directly from the data subjects themselves. A data protection notice must accompany any request for personal data. Any employees responsible for managing the collection of personal data for the legitimate activities of the MIoD must ensure that a notice containing the following information is included in the request for that data:

7.1.1. A statement that the MIoD is the data controller.

7.1.2. The names and contacts of the Designated Data Controller(s).

7.1.3. A clear explanation of the types of data being collected and the purposes for which that data will be processed.

7.1.4. Any further information that is considered necessary to ensure that the data processing can be described as transparent, for example details of any third parties to whom the data might be disclosed.

7.1.5. A statement making it clear that by submitting the personal data, the data subjects are giving their consent for the processing of the data for the stated purposes to take place.

8. **Data Security**

8.1. Of fundamental importance within any data protection regime is the security of the personal data that is being processed. Data subjects have the right to expect that their personal data will be kept and processed securely and that no unauthorised disclosures or transfers will take place to anyone either within or outside of the MIoD without their permission. Authorised disclosures or transfers are those that are declared to the data subject either at the point of data collection or subsequently, the necessary consent for disclosure or transfer having been obtained if required.

8.2. All employees are responsible for ensuring that:

- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

8.3. Each member of staff whose work involves storing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage, in line with the MIoD's Data Protection and Retention Policy.

8.4. Employees should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

9. **Safekeeping of information**

9.1. Personal information should:

9.1.1. Be kept in a locked filing cabinet, drawer, or safe; *or*

9.1.2. If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; *and*

9.1.3. If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

10. **Secure processing of personal data**

10.1. While employees in the course of performing their legitimate duties are using personal data, reasonable precautions must be taken to ensure the safety and privacy of that data. For example:

10.1.1. In open-plan offices, computer screens that could potentially be displaying personal data should not be positioned such that unauthorised persons may readily see that data, and password protected screen savers should be used.

10.1.2. Personal data in manual form, such as in paper files, correspondence or database printouts, should not be left in view in open-plan offices while the relevant staff members are away from their desks. They should instead be locked away or at least covered.

10.1.3. Where manual records containing personal data are accessible to a number of employees they must not be removed from the office and should always be returned at the end of the day to their proper place.

10.1.4. Ordinarily, personal data should not be processed at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the same precautions should be taken by employees as if they were working in the privacy of the MIoD office.

11. **Authorised and unauthorised disclosures**

11.1. Employees working with personal data must be made aware of the purposes for which the data is processed and the legitimate parties either within or outside the MIoD to whom that data, either in whole or in part, may be disclosed or transferred.

11.2. Personal information must not be disclosed either orally or in writing or via Web pages or by any other means, manual or electronic, accidentally or otherwise, to any unauthorised third party.

11.3. Ordinarily, personal data should never be stored at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites, unless as part of the company's business continuity procedures or without written permission.

11.4. Employees should be aware that log files would record details of all users who access, alter or delete or attempt to access, alter or delete centrally held computerised databases and files containing personal data.

11.5. Employees should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

12. **Security of data during transfer**

12.1. Where personal data is transferred between employees within the MIOD in the course of their legitimate activities, employees should be aware of the sensitive nature of such data and ensure the appropriate level of security.

13. **Disclosures outside the MIoD**

13.1. When a request to disclose or amend personal data relating to an employee or member of the MIoD is received from an individual or organisation outside the MIoD, in general no data should be disclosed or amended unless the authority and authenticity of the request can be established. Disclosures requested by those claiming to be relatives or friends should be refused unless the consent of the data subject is obtained for such disclosures or in one of the few situations where disclosure without consent is permitted by the law.

13.2. Requests for the disclosure of personal data from the Police, Government bodies, or other official bodies and agencies should be investigated sufficiently to verify the authenticity of the request and may then be acted upon if there is a legal requirement for such disclosure or the consent of the data subject has been given for the disclosure.

13.3. In all cases the permission of the Designated Data Controller is required.

14. **Amendment of personal data**

14.1. From time to time data subjects will wish to update some of their personal data held by the MIoD, for example their home addresses or other contact details previously submitted. To do this, the data subjects must provide the MIoD with their updated data and the MIoD employee handling this data must satisfy themselves that of the proof of identity of the data subject.

14.2. With the introduction of MIoD 'self-service' web-based administrative systems for employees and members, the data subjects themselves are able to take responsibility for the maintenance of certain elements of their personal records. Where company "Superusers" are given the ability to manage their employees' profiles and data, the permission of the employee must first be obtained.

14.3. These systems incorporate the necessary authentication and security mechanisms to ensure that data subjects are only able to view and amend their own data.

15. **Subject Consent**

15.1. (see S 24 of the Act) The MIoD can only process personal data with the express consent of the individual save for in some specific situations as set out in Section 24(2) of the Act. Eg the MIoD may ask employees for information about particular health needs, or any medical condition. The MIoD will only use this information in the protection of the health and safety of the individual, but will need the employee's consent to process this data in the event of a medical emergency, for example.

15.2. Therefore, employees will be asked to complete a form requesting permission to process their personal data in the event of a medical emergency or for a specified purpose eg company pension or health plan

16. **Publication of MIoD Information**

16.1. The names and some biographical information of Board Directors, Employees, Trainers and members of the MIoD may be published in the Annual Report and on the MIoD's public Web site and Newsletter and in any other documents where any statute or law requires such data to be made public.

Retention of Data

16.2. The MIoD has a duty to retain some employee and member personal data for a period of time following their departure or resignation from the MIoD, mainly for legal reasons, but also for other purposes such as financial reasons, for example relating to pensions and taxation. Information held by the MIoD will be retained as long as the purpose for which the information was collected continues. The information is then destroyed unless its retention is required to satisfy legal, regulatory or accounting requirements or to protect the MIoD's interests. As a general rule, the maximum retention period is 7 years.

The table below sets specific retention requirements:

Document	**Minimum Retention Requirement**
Accounting records	7 years
Contracts and leases	7 years or until dated of expiry of contract/lease whichever is the latest
Company records (specified in Section 190 of the Companies Act)	7 years
Employment applications and interview sheets	6 months
Membership application (where hard copies are received)	1 year
Insurance records, current accident reports, claims , policies, and the like	7 years or until dated of expiry of policy whichever is the latest
Payroll records and summaries	7 years
Personnel files (terminated/resigned employees)	7 years
Retirement records	Permanently
Documents related to Mauritius Qualifications Authority	7 years
Trademark registrations and copyrights	Permanently

16.3. While the majority of personal data held by the MIoD is processed for internal administrative purposes and is never disclosed outside the institute, some

categories of data are routinely or from time to time released through one or more forms of publication such as:

- MIoD Website
- MIoD Newsletter
- Annual Report
- Directors' Register
- Disaster Recovery and Business Continuity Plan

16.4. Data subjects are informed of the MIoD's obligations or policy in this respect at the time the data is collected.

17. **Disposal of personal data**

17.1. When a record containing personal data is to be disposed of, the following procedures will be followed:

17.1.1. All paper or microfilm documentation containing personal data will be permanently destroyed by shredding or incinerating, depending on the sensitivity of the personal data.

17.1.2. All computer equipment or media that are to be sold or scrapped will have had all personal data completely destroyed, by re-formatting, over-writing or degaussing.

17.2. Employees will be provided with guidance as to the correct mechanisms for disposal of different types of personal data. In particular, employees will be made aware that erasing/deleting electronic files does not equate to destroying them.

18. **Subject Access Requests**

18.1. All staff and members have a right to access certain personal data being kept about them at the MIoD either on computer or in certain files.

18.2. All employees and members are entitled to know:

18.2.1. what information the MIoD holds and processes about them and why

18.2.2. how to gain access to it

18.2.3. how to keep it up to date and

18.2.4. what the MIoD is doing to comply with its obligations under the Act

18.3. The MIoD will, upon request, provide all employees and members with a statement regarding the personal data held about them. This will state all the types of data the MIoD holds and processes about them, and the reasons for which they are processed.

18.4. Any person who wishes to exercise this right should complete the Request Form and submit it to the appropriate Designated Data Controller (see above). The MIoD aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 14 days.

18.5. Request to access personal data may be denied where:

18.5.1. the MIoD is not supplied with such information as it may reasonably require in order to satisfy itself as to the identity of the person making the request and to locate the information which the person seeks;

18.5.2. compliance with such request will be in contravention with its confidentiality obligation imposed under any other enactment.

18.6. Where as a result of complying with a request to access personal data, the MIoD would have to disclose personal data relating to another person, it may refuse the request unless:

18.6.1. the other individual has consented to the disclosure of his personal data to the person making the request; or

18.6.2. he obtains the written approval of the Designated Data Controller (in this case being the CEO).

18.7. The MIoD shall not comply with a request to access personal data where –

18.7.1. it is being requested to disclose information given or to be given in confidence for the purposes of:

a) the education, training or employment, or prospective education, training or employment, of the data subject;

b) the appointment, or prospective appointment, of the data subject to any office; or

c) the provision, or prospective provision, by the data subject of any service;

18.7.2. the personal data requested consists of information recorded by candidates during an academic, professional or other examination;

18.7.3. such compliance would, by revealing evidence of the commission of any offence other than an offence under the Act, expose him to proceedings for that offence.

19. **Processing of Personal Data within the MIoD Activities**

19.1. Listed below are the activities carried out within the MIoD that involve the processing of personal data. This list is non exhaustive and it is the responsibility of the CEO to ensure that all employees receive sufficiently detailed guidance to enable them to carry out these activities in accordance with the requirements of the Data Protection Act and the MIoD Data Protection and Retention Policy.

19.2. Membership applications and management

19.3. Directors Register

19.4. General enquiries

19.5. Events/conference administration

19.6. Publications eg Website, Newsletter, Annual Report

19.7. Marketing incl fundraising activities/donor administration etc

19.8. Research activities and administration
19.9. Staff management (includes performance, appraisal and development records, leave
19.10. Records, expenses records, etc
19.11. Staff recruitment
19.12. Systems administration (e-mail, back-up/ storage, authentication, system logs, etc)
19.13. Trainers, facilitators and presenters activities and administration
19.14. Finance administration (includes payroll, banking, tax, pensions)
19.15. Health and Safety
19.16. CRM and Mailing list administration and use
19.17. Market research
19.18. News/press release activities/public relations and other publication activities

20. **Conclusion**

20.1. Compliance with the Data Protection Act is the responsibility of all the employees of the MIoD. Any deliberate breach of the MIoD Data Protection and Retention Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

20.2. Any questions or concerns about the interpretation or operation of this policy should be taken up with the appropriate Designated Data Controller.

Request Form

1. Details of the person requesting the information.	
Full name:	
Address:	
Telephone number:	
Fax Number:	
Email:	
2. Are you the Data Subject?	YES/NO
(a) **IF YES PLEASE COMPLETE THIS SECTION. ELSE PROCEED TO SECTION (b)**	
If you are the Data Subject please supply evidence of your identity i.e. ID card or Passport.	
Please tick appropriate box	
I am a current/former member of staff	

I am a current/former member	
I am neither of the above	
Please now go to question 5.	
(b) **IF NO**	
Are you acting on behalf of the Data Subject with their written authority? If so, that authority must be enclosed.	
Please also state the relationship of the Data Subject to the MIoD:	
The Data Subject is a current/former member of staff	
The Data Subject is a current/former member	
The Data Subject is neither of the above	
Please now go to questions 3 and 4.	
3. Details of the Data Subject (if different from 1.)	
Full name:	
Address:	
Telephone number:	
Fax Number:	
Email:	
4. Please describe your relationship with the Data Subject that leads you to make this request for information on their behalf.	
5. If you wish to see only certain specific document(s), please describe thes.	
6. If you would like a more	

general search, please note that the MIoD is able to search the following sections for personal data. Please indicate the sections that you would like searched:	
• Members Register	
• Directors Register	
• Human Resources	
• Finance	
• Administrative files and information	
• Other	
7. Declaration	
I, ……., certify that the information given on this application form is true. I understand that it is necessary for the MIoD to confirm my/the Data Subject's Identity and it may be necessary for more detailed information to be obtained in order to locate the correct information. **Signed:……** **Date:…….**	
Please return the completed form to the MIoD at the following address:	
1st Floor, Raffles Tower, 19 Cybercity, Ebene or send by email to contact@miod.mu	

Glossary	Annex 1
“collect”	does not include receipt of unsolicited information;
“computer”	means any device for storing and processing information, whether or not the information is derived from other information by calculation, comparison or otherwise;
“consent”	means any freely given specific and informed indication of the wishes of the data subject by which he signifies his agreement to personal data relating to him being processed;
"data"	means information in a form which – (a) (i) is capable of being processed by means of equipment operating automatically in response to instructions given for that purpose; and (ii) is recorded with the intent of it being processed by such equipment; or (b) is recorded as part of a relevant filing system or intended to be part of a relevant filing system;
"data controller"	means a person who, either alone or jointly with any other person, makes a decision with regard to the purposes for which and in the manner in which any personal data are, or are to be, processed;
“data matching procedure”	means any procedure, whether manually or by means of any electronic or other device, whereby personal data collected for one or more purposes in respect of 10 or more data subjects are compared with personal data collected for any other purpose in respect of those data subjects where the comparison – (a) is for the purpose of producing or verifying data that; or (b) produces or verifies data in respect of which it is reasonable to believe that it is practicable that the data, may be used, whether immediately or at any subsequent time, for the purpose of taking any adverse action against any of those data subjects;
"data processor"	means a person, other than an employee of the data controller, who processes the data on behalf of the data controller;
"data protection principles"	means the data protection principles specified in the First Schedule;
"data subject"	means a living individual who is the subject of personal data;
“direct marketing”	means the communication of any advertising or marketing material which is directed to any particular individual;
“document”	includes – (a) a disc, tape or any other device in which the data other than visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the disc, tape or other device; and (b) a film, tape or other device in which visual images are embodied as to be capable, with or without the aid of some other equipment, of being reproduced from the film, tape or other device;

“information and communication technologies”	“information and communication technologies” – (a) means technologies employed in collecting, storing, using or sending out information; and (b) includes those involving the use of computers or any telecommunication system;
“inaccurate”	in relation to personal data, means data which are incorrect, misleading, incomplete or obsolete;
“individual”	“means a living individual;
"personal data"	means - (a) data which relate to an individual who can be identified from those data; or (b) data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion;
"processing"	"processing" means any operation or set of operations which is performed on the datawholly or partly by automatic means, or otherwise than by automatic means, and includes (a) collecting, organising or altering the data; (b) retrieving, consulting, using, storing or adapting the data; (c) disclosing the data by transmitting, disseminating or otherwise making it available; or (d) aligning, combining, blocking, erasing or destroying the data;
"sensitive personal data”	means personal information concerning a data subject and consisting of information as to - (a) the racial or ethnic origin; (b) political opinion or adherence; (c) religious belief or other belief of a similar nature; (d) membership to a trade union; (e) physical or mental health; (f) sexual preferences or practices; (g) the commission or alleged commission of an offence; or (h) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings;
“third party”	in relation to personal data, means any person other than – (a) the data subject; (b) a relevant person in the case of a data subject; (c) the data controller; or (d) a person authorised in writing by the data controller to collect, hold, process or use the data – (i) under the direct control of the data controller; or (ii) on behalf of the data controller;
“use”	in relation to personal data, includes disclose or transfer the data.


MIoD
Mauritius
Institute of
Directors