UNIVERSITY OF MAURITIUS

DATA PROTECTION POLICY

2023

October 2023

1. Definitions

In this policy, the following definitions apply:

- **Act:** The Data Protection Act 2017, which is the law governing the protection of personal data in Mauritius.
- **Consent:** Any freely given specific, informed and unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmative action, by which he signifies his agreement to personal data relating to him being processed.
- **Data Subject:** An identified or identifiable individual, 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, physiological, genetic, mental, economic, cultural or social identity of that individual.
- **Data processing:** 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.
- **Data Protection Commissioner:** The Head of the Data Protection Office who shall be a Barrister of not less than 5 years' standing.
- **Data Controller:** A person who, or a public body which, alone or jointly with others, **d**etermines the purposes and means of the processing of personal data and has decision making power with respect to the processing.
- **Data Processor:** A person who, or a public body which processes personal data on behalf of and according to the purposes defined by the data controller.
- **Digital Archive:** The designated repository in which digital records are retained for their long term preservation.
- **Records:** Records of personal data can be both digital and non-digital. In case where personal information is recorded in digital form, it then requires a computerised system to access or process.
- **Personal Data:** Any information relating to a data subject and/or information or an expression of opinion that identifies or may permit an individual to be identified..
- **Special Categories of personal data (including Sensitive Personal Data):** In relation to a data subject, means personal data pertaining to:

  a) his racial or ethnic origin;
  b) his political opinion or adherence;
  c) his religious or philosophical beliefs;
  d) his membership of a trade union;
  e) his physical or mental health or medical condition;
  f) his sexual orientation, practices or preferences;
  g) his genetic data or biometric data uniquely identifying him;
  h) the commission or alleged commission of an offence by him;
  i) 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 the proceedings; or
  j) such other personal data as the Commissioner may determine to be sensitive personal data.

2. Policy Statement

The **University of Mauritius** (also referred to as '**UoM**') commits to comply with the provisions of the **Data Protection Act 2017** (also referred to as 'The Act').

As a tertiary education institution, an employer and a service provider, UoM shall be committed to:

- processing data fairly and legally;
- safeguarding the fundamental rights of individuals;
- keeping personal data secure; and
- designing and incorporating privacy into systems and processes.

This Data Protection Policy sets out the guidelines and procedures adopted at UoM for data protection.

3. Scope

UoM is registered as a Data Controller with the Data Protection Commissioner's Office, as per the Act. This allows the UoM to control data associated with its academic and research activities, administrative functions and processes, library services and any other business services. UoM determines the purposes and means of the processing of personal data and has decision making power with respect to such processing.

The policy applies equally to full time and part time employees on a substantive or a fixed-term contract and to associated individuals who work for UoM including agency staff, contractors, and others employed under a contract of service.

4. Purposes and Objectives

The purpose of this policy is to:

- Assist UoM to meet its legal obligations under The Data Protection Act 2017;
- assist UoM staff in fulfilling their responsibilities with respect to the processing of personal data in compliance with the legal and regulatory framework in force; and
- ensure accountability for retaining certain personal data for as long as is required. While treating personal data, UoM shall not keep such data for any longer than is necessary.

5. Principles

In accordance with the Act, UoM has the obligation to and shall process data according to the data protection principles, as set out in the following table:

Principles	Application of the principles by UoM
Lawfulness, fairness, and transparency	UoM explains to its staff, students, suppliers and other stakeholders how it processes personal data at the point of collection and for what purposes.
Purpose limitation	UoM uses the personal data it has only for the specific purpose that it was collected.
Data minimisation	UoM only collects personal data which is adequate, relevant and not excessive in relation to the purpose for whichi it is processed..
Accuracy	UoM ensures that the data is accurate, updated and is able to rectify any mistakes at the earliest.
Storage Limitation	UoM does not retain personal data for longer than needed, for the purposes for which the personal data is processed and in accordance with the data subject's rights
Integrity and Confidentiality	UoM protects all personal data collected against unauthorised access, loss or damage by a range of security measures.

6. Collection of Personal Data

The collection of personal data shall be driven by a lawful purpose connected with a function or activity of the UoM and where such collection shall be warranted and necessary for that purpose.

Upon collection of data, UoM shall ensure that the data subject be informed of:

- the identity and contact details of the Controller and, where applicable, its representative and any Data Protection Officer (as per paragraph 21 of this policy);
- the purposefor which the data are being collected;
- the intended recipients of the data;
- whether or not the supply of the data by that data subject is mandatory or voluntary (voluntary data shall be marked as 'optional' on the relevant form);
- the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

- the retention period applicable (paragraph 7 of the policy shall prevail);
- any further information necessary to guarantee fair processing in respect of the personal data collected.

The types of data collected at UoM, from data subject are of the following nature:

1. Name;
2. Residential address;
3. Telephone number;
4. E-mail address;
5. Date of birth;
6. Gender;
7. Identity number;
8. Marriage/civil status;
9. Photo;
10. Salary;
11. Qualification;
12. Medical record;
13. Reference;
14. Results and transcript of examination;
15. Assignment;
16. Bank detail;
17. Parents/Guardian' detail;
18. Examination paper/script; and
19. Social Background.

The list is not an exhaustive one.

7. Data Processing and Data Disclosure

The data collected is processed on the basis of the data subject's consent and for the purposes as described in the following two tables at Paragraphs 7.1 and 7.2. In certain circumstances, in line with the Act, UoM may also allow personal data to be shared among public sector agencies without the consent of the data subject.

7.1 Legal Basis for Processing - Personal Data

UoM shall ensure that it processes personal data on one of the following basis:

Legal basis	Contextual Application
Necessary for the performance of a contract	The majority of processing for UoM students, staff and suppliers.
Data subject has given consent to the processing	Mailing lists, marketing and other optional services for staff, students and other stakeholders.
Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	Retention of students' results list, transcript information for award and verification, and information, regarding staff members, sent to the Mauritius Revenue Authority (MRA).
Necessary for the purposes of legitimate interests pursued by the UoM or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data	Activities involving students, alumni, charitable works and marketing of commercial services for UoM.
Necessary for the performance of contract, historical, statistical or scientific research	Civil Service Mutual Aid Association requesting information on staff; University monitoring of student progress and achievement; Organisations wishing to recruit UoM graduates or students for placements.

7.2 Legal Basis for Processing - Special Categories of Personal Data

UoM shall process special categories of personal data on the following basis:

Legal basis	Contextual Application
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.	Absence due to sickness Notification of Trade Union membership Examination results References
Relating to personal data which are manifestly made public by the data subject	For research purposes (Alumni research); or Particular group donation assessments
Necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee	Occupational therapy assessments Doctors' reports and records
Necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes	Analysis and reporting of equality and diversity information, research outcome and the impacts on society and the country, the employability of the graduates

8. Retention of Personal Records

UoM shall retain the personal data of employees and other members for a period of time as referred to in the Data Retention Schedule at paragraph 8.1. The retention will be effective following the member's departure or resignation from UoM and will be governed by legal and financial considerations.

Data held by UoM shall be retained as long as the purpose underlying the collection of the data continues. Upon expiry of the purpose, the data shall then be destroyed; unless its retention is required to satisfy legal, regulatory or accounting requirements or to protect the interests of UoM.

Under this policy, the nature of the records requires that consideration be given to:

- security;
- authenticity;
- accessibility;
- version control; and
- preservation (e.g. back-up of digital records).

The records identified for destruction **shall not be recoverable**.

8.1 Data Retention Schedule

The Act does not provide for a specific time period for retaining personal data. The provisions indicate that personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Some Personal Data may need to be held for longer periods than others.

From this perspective, a Data Retention Schedule will provide the guidance on how long different categories of records are to be held and when same may be destroyed. Once the retention periods have elapsed, all records shall be destroyed, unless defined as permanent preservation.

All documents are to be held permanently except for the ones which are enumerated in the table below. The table describes the retention periods as applicable to the different classes of documents which relate to the data collected and processed.

Sn	Class of Documents Containing Personal Data	Timeframes
1	Documents relating to previous freehold ownership of property	Ten (10) years after ownership has been transferred
2	Any expired lease agreements	Ten (10) years subject to there being no litigation; otherwise ten (10) years after litigation has ended
3	Agreements with periodic payment	Ten (10) years subject to there being no litigation; otherwise ten (10) years after litigation has ended
4	Banking documents and all financial statements	Ten (10) years after utilisation
5	Unsuccessful application to undergo any courses at the UoM; except for reason of fraud or previous misconduct at UoM	Twelve (12) months as from date of the decision communicated subject to there being no litigation; otherwise three (3) years after litigation has ended
6	Unsuccessful job application; except for reason of fraud or previous misconduct at UoM	Twelve (12) months as from the date the application has been unsuccessful; except where there is an ongoing litigation/dispute regarding the application

Note:

- Documents which have nothing to do with personal information, such as course guidelines, syllabi, workshop documents, are not governed by the Data Protection Act.
- Documents that are to be destroyed as per the policy should have the approval of the National Archives Department under the National Archives Act 1999.
- The generality of the approach of the Retention Schedule aims at an increased accessibility and usability among members of UoM.
- For Finance issues, the Retention Schedule shall be in line with the Financial Management Manual.
- Destruction of any data should be approved by the UoM Council, prior to any destruction of the same.

8.2 Retention of Personal Data of Students

The time frame for retention of personal data of students shall be maintained to the minimum allowed, which shall aid in the management of large stores of data.

The underlying considerations with respect to students' personal data handling are:

- Long term records - The classification as 'Long Terms Records' results from the fact that life of student is counted as being 120 years from the date of birth;
- There is an expectation by students, employers, Government Bodies and members of the public that Universities should retain a permanent core record of student names, the modules studied, qualifications and the outcomes;
- Data required for management, development and research may be retained outside the student records systems for the long term. When storing this data, the name and address of a student will be removed and in line with the Act, the data will not be used to support any actions or decisions that affect or cause distress or damage to the individual. The exception will be research data which requires the student's agreement for follow-up contact.

9. Rights

Data subjects (UoM students, staff, customers, suppliers and other stakeholders) have a number of rights under the Act. These include:

Rights	The context for UoM
Right of access	Data subjects have the rights to find out what the UoM is doing with their data, check whether the data is held correctly and to obtain a copy thereof.
Rights to rectification	UoM shall endeavour to ensure that the data held is accurate. It shall also provide the opportunity to data subjects to request rectification of their personal data in the event that the data is incorrect. Subject to provisions of Section 39(4) of the Act, UoM shall make the necessary amendments without undue delay.
Right to erasure	A Data subject has the right to ask UoM to remove or delete data held on him/her. After consideration of a request from a data subject, UoM will proceed with any erasure of data held, in line of section 39 of the Act.
Right to restriction of processing	Data subjects may, in the course of a dispute with UoM about the use of their data, request UoM to stop using their data if certain criteria apply. The UoM, as Controller shall, at the request of a data subject, restrict the processing of personal data where: 1. The data subject challenges the data accuracy; 2. The Controller no longer needs the personal data for the purpose of the processing, but the data subject requires them for the establishment, exercise or defence of a legal claim; 3. The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or 4. The data subject has objected to the processing pursuant to section 41 of the Act, pending verification as to whether the legitimate grounds of the Controller override those of the data subject.
Right to object	Data subjects have the right to object to processing. The relevant grounds of objection shall be based on legitimate interests, legal obligation or for the purposes of direct marketing or for "scientific or historical research purposes or statistical purposes", UoM will assess the request against any compelling legitimate grounds for the processing and respond accordingly.

Automated decision making, including profiling	Data subjects hold a right of appeal against decisions of UoM, with regards to the data subjects and which have been taken through automated means such as computer algorithm. UoM shall ensure a fair treatment of the data subjects, allowing them the opportunity to express their point of view. Further, UoM shall delegate a member of staff to provide a review and explanation of the decision to the data subject.

Data subjects shall thus have the right to access their data, to obtain a copy of the data held, to request its erasure or rectification and the right not to be subject to a purely automated decision without having their views taken into consideration. The data subjects also has the right to object to processing, withdrawing their consent and lodging a complaint with the Data Protection Office should they consider that the processing is in violation with the law.

10. Data Security

UoM is committed to ensuring the security of personal data in order to prevent unauthorised access, accidental deletion and malicious hacking attempts.

UoM's overarching IT policy supports compliance around the 'Integrity and Confidentiality' principles of the regulation, in ensuring that appropriate technical measures are in place to protect personal data.

Documents containing personal data should be encrypted or password protected as per the IT Policy and CITS guidelines in place at all times.

In the event of a personal data breach:

- The Data Protection Officer shall be contacted without delay for immediate action; and
- In case such an officer is not in place and/or not available, the Data Protection Commissioner should be informed of the breach within 72 hours.

11. Data Protection by Design

UoM is committed to ensure that privacy is built into its processes and outcomes. New projects involving personal data are required to carry out a data protection impact assessment. The data protection impact assessment aims to identify privacy risks and plan appropriate mitigation.

12. Data Protection Impact Assessment

The Act provides for the instrument for a data protection impact assessment (DPIA). This refers to the obligation of the controller to conduct an impact assessment and to document it before starting the intended data processing. Such an assessment may bundle several processing procedures.

A DPIA shall always be conducted where processing operations are likely to result in a high risk to the rights and freedoms of data subjects by virtue of their nature, scope, context and purposes.

13. Training and Awareness

UoM is committed to ensure that its staff have the requisite training and awareness on data protection. All members of the staff are required to undertake the compulsory 'Data Protection' training.

Further resources and training are provided on the intranet and on request from the Data Protection Officer. Breach of data protection law due to unauthorized access, misuse or loss may result in disciplinary action, including dismissal.

14. Using Data Processors

UoM may use an external contractor or 'data processor' to store or manage its data. Such Data Processor will process this data only for purposes specified by UoM and will be bound by contract to meet UoM's obligations under the Act.

15. UoM as Processor

Where UoM acts as a processor in the course of its academic research and/or commercial activities, it shall:

- process the personal data only on documented instructions from UoM;
- ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- take all measures required regarding the security of processing;
- not engage another processor without prior specific or general written authorisation of the controller;
- assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights; and
- make available to the controller all information necessary to demonstrate compliance.

16. Academic Research

Academic research which involves the processing of personal data is subject to Section 28 of the Act and any other policy and contractual obligations. As per the Act, it is important to request for the consent of students before using their personal information to carry out any academic research.

17. Responsibilities of UoM Employees for Managing University Records

Operational responsibility for the implementation of this policy rests upon the Head of each Department/Section of UoM.

Each Department/Section shall be called upon to:

- abide by this policy;
- ensure that all Records Management practices are consistent with this policy;
- destroy inactive records that have no archival value upon expiry of the applicable retention period;

Additionally, each Faculty/Department/Centre/Office/Unit shall have to ensure that the appropriate security measures are observed for maintaining records containing personal or other confidential information. The confidentiality of information within records must be safeguarded at all times.

Once records have been retained by the creating offices for the requisite time as stipulated in the attached retention schedule, they must be destroyed or archived for permanent retention as set out below:

- When scheduled for destruction, records must be disposed of securely. The manner of destruction of records must be appropriate to the level of confidentiality of the records;
- In the case of in-house destruction, the department/section should document and retain the date and manner of destruction of records;
- In the case of third-party destruction, a certificate confirming destruction should be received and retained as proof of destruction.

18 . Links to Another Website

The website of the UoM may contain links to other websites of interest. However, once these links have been used to leave the site, UoM shall not have any control over the other website. Therefore, UoM cannot be responsible for the protection and privacy of any information which data subjects provide while visiting such sites. Such websites are not covered by this policy.

19. Use of CCTV

The use of CCTV systems have to comply with the provisions of The Data Protection Act 2017 as elaborated under the UoM Data Protection Policy for CCTV systems.

20. Non-Compliance under the Policy

Deliberate failure of employees to comply with this Policy may entail disciplinary action.

21. The Data Protection Officer

In accordance with the Act, UoM has appointed a Data Protection Officer. The Contact Details of the UoM Data Protection Officer are mentioned hereunder:

Me. Sivaramen SUBBARAYAN
Legal Affairs Director and Data Protection Officer
University of Mauritius
The Core,

Ebene

TEL: (230) 463 8051
Email: dla@uom.ac.mu

22. Request Procedure

Requests made under this policy are to be sent to the Data Protection Officer. A reply to the request shall be due within one month.

This period may be extended by a further period of two months in cases where:

- the request bears a high complexity case; or
- a heavy influx of requests is being processed.

Any such extension will be notified to the requestor.

23. Conclusion

This policy has been developed in line with the requirements of The Data Protection Act 2017 which complies with the General Data Protection Regulations (GDPR).

The Policy is to be reviewed every two years in the light of the changes in UoM operations. Further it may be updated as and when required to reflect the best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Act and other existing laws.

Disclaimer

This policy is for general guidance only. It does not include all possible situations and it cannot substitute the Law or take the place of legal advice. Readers are advised to consult the DPA 2017 and to seek legal advice in case of doubt.

The UoM will not bear any responsibility for any legal damages arising from action or absence of action of any person on account of the contents of the policy.