Policy Title	Privacy Preservation Policy
Responsible AIU Office (Higher Management/Directorate)	Chief Information Officer (CIO)
Policy Owner (Executive Department/Office)	IT Security Office
Pertinent Dates	July 2022

I. SCOPE OF POLICY

This policy affirms AIU's commitment to privacy and its approach to the responsible handling of personal, sensitive and health information in all its forms, consistent with relevant legislation.

This policy applies to all staff, students, researchers and affiliates of the AIU including contractors and partners providing services on behalf of AIU**.**

II. DEFINITIONS

Personal data - Refers to any information relating to an identified or identifiable natural person, directly or indirectly, 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 natural person.

Personal information - Information or an opinion, that is recorded in any form about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. Typically, this includes information like name, date of birth, address, phone number etc. Personal information includes personal data.

Sensitive information - A special category of personal information that requires more protection. It includes the following information about an individual: racial or ethnic origin; political opinion; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; criminal record.

III. POLICY STATEMENT

AIU values the privacy of individuals and will foster a positive and respectful privacy culture which supports a relationship of trust between AIU and staff, students, researchers and third parties.

AIU has an obligation to provide accurate, reliable information to authorized recipients and to preserve vital records. MIT is increasingly dependent on the accuracy, availability, and accessibility of information stored electronically and, on the computing, and networking resources that store, process, and transmit this information. Records created and maintained in electronic form are included in the universities's

definition of archival materials. In addition, records must sometimes be preserved for prescribed periods of time for litigation or other legal purposes.

Members of the AIU community should exercise caution to protect information (and particularly personal information) from unauthorized disclosure. Particular caution should be used with electronic communications, because of the ease with which such communications can be distributed and due to concerns about unauthorized access. Unauthorized interception of email and other electronic communications is prohibited by AIU policy and may also violate state and federal law.

IV. RESPONSIBILITIES

Privacy is everyone's responsibility and all staff, students, researchers and affiliates have an obligation to manage personal information collected, accessed, used, re-used or disclosed during their engagement with AIU in accordance with this policy, the AIU Privacy Statement, and associated information security, information management and data governance policies.

- Managers are required to ensure that privacy principles and practices are implemented locally, and suspected or actual breaches of this policy are reported in accordance with the Compliance Breach Management Procedure.

- The Privacy Office is responsible for:

    - establishing the privacy management framework to enable communication and implementation of applicable privacy requirements
    - reviewing privacy impact assessments
    - providing privacy training, other education programs and advice
    - monitoring compliance with this policy and reporting on complaints and breaches of this policy to internal governance bodies and external agencies, as required
    - investigating privacy breaches, incidents or complaints
    - appointing a Chief Privacy Officer who issues and maintains the AIU Privacy Statement and core collection statements
    - providing a central contact point for and on behalf of the AIU Group.

(14) The Chief Information Security Officer oversees information security controls and responses to enable AIU to deliver effective protection of personal data held by AIU consistent with privacy management obligations across all its operations.

(15) The Chief Financial Officer is responsible for making determinations on external reporting on the recommendation of the Chief Privacy Officer or Chief Audit and Risk Officer, in the event of a privacy breach.

(16) The Privacy Office monitors compliance with this policy and reports on complaints and breaches of this policy to internal governance bodies and external agencies, as required.

V. POLICY STANDARDS AND PROCEDURES

Any member of the AIU community who accesses information from records maintained by another individual without the individual's consent must seek prior approval from the applicable Senior Officer or his or her designee for such access and related disclosure; the Senior Officer or designee may consult the Chief Information Officer. This process applies to requests for access from an outside entity or from another office within AIU.

VI. FORMS/INSTRUCTIONS (if applicable)

N/A

VII. APPENDICES (if applicable)

N/A

VIII. RELATED POLICIES

Information Security Policy

VIV. CONTACT INFORMATION

Chief Information Officer (CIO)

Triggered by:	Name	Date	Sig.
Created by:	Name	Date	Sig.
Revised by:	Name	Date	Sig.
Approved by:	Name	Date	Sig.