DATA PROTECTION POLICY

1. INTRODUCTION

1.1. The African Leadership College (ALC) needs to create, collect, process and retain certain information about its employees, workers, students, clients and other individuals for various purposes. These purposes include managing the progress of students, managing staff, recruiting and employing staff and complying with legal and statutory regulations. ALC is committed to protecting the rights and freedoms of individuals in respect of managing the personal information that it processes.

1.2 This Policy sets out responsibilities and actions that ALC will take to meet this commitment in accordance with our obligations and ensure compliance with the Mauritius Data Protection Act 2017 (DPA 17) and the General Data Protection Regulation (GDPR).

1.3 This Policy applies to all staff, students and lay governors and all personal data that are created, collected, stored and processed through the activity of the institution and where ALC is the Data Controller. It also sets out the responsibilities of the institution, its staff and its students to comply with the provisions of GDPR and DAP 17.

2. DATA PROTECTION PRINCIPLES

ALC shall comply with the Data Protection Principles set out in the DPA 17. In summary these state that:

2.1 Personal data shall be processed fairly and lawfully.

2.2 Personal data shall be obtained only for specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose.

2.3 Personal data shall be adequate, relevant and not excessive in relation to the purpose for which they are processed.

2.4 Personal data shall be accurate and, where necessary, kept up to date.

2.5 Personal data processed for any purpose shall not be kept longer than is necessary for that purpose or those purposes.

2.6 Personal data shall be processed in accordance with the rights of the data subjects under both the DPA (Data Protection Act) and General Data Protection Regulation (GDPR).

2.7 Appropriate security and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. H. Personal data shall not be transferred to another country, unless that country ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data.

3. DEFINITIONS

3.1 Data Subject - Identified or identifiable natural person.

3.2 Personal data - 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, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.3 Data Controller - An individual or legal person, public authority, agency or other body who determines the purposes and means of processing personal data.

3.4 Data Processor - An individual or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

3.5 Special Categories of Data - Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Information relating to criminal convictions and offences are not included but should be offered the same level of protection.

3.6 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.

3.7 Anonymisation - The process of turning data into a form which does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information.

3.8 Profiling - Automated processing of personal data to evaluate certain things about an individual.

3.9 Pseudonymisation - Procedure by which the most identifying fields within a data record are replaced by one or more artificial identifiers or pseudonyms.

3.10 Automatic decision-making - Making a decision solely by automated means without any human involvement.

3.11 Data Protection Impact Assessment (DPIA) - An assessment which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

3.10 Direct Marketing - The communication (by whatever means) of any advertising or marketing material which is directed to particular individuals. This covers all advertising or promotional material, including that promoting the aims or ideals of not-for-profit organisations for example, it covers a charity or political party campaigning for support or funds.

4. ROLES AND RESPONSIBILITIES

4.1 Staff Roles and Responsibilities

4.1.1 All staff shall be individually responsible for ensuring that the processing of personal data is in accordance with University policy and guidelines.

4.1.2 Deans and Heads of Department shall be responsible for ensuring that their teams adopt and conform to this Policy.

4.1.3 Members of staff must include appropriate Data Protection statements on all documents that are used to collect personal information e.g. Student Registration Forms, Staff Contracts, etc. These statements must include informing the data subject of information being collected, its purpose and to whom it may be disclosed.

4.1.4 Members of the Senate Research & Ethics Committee and staff supervising student work must ensure that the students adhere to this Policy when processing personal information.

4.1.5 A Data Protection Officer (DPO) shall be accountable for the implementation and management of this Policy.

4.1.6 ALC will maintain a record of processing activities which records information relating to the processing of personal data carried out.

4.1.7 ALC will maintain an Information Asset Register (IAR) to capture these requirements which include: the purpose of the processing, the types of individuals about which information is held, who personal information is shared with and when personal information is transferred to other insitutitions outside of ALC.

4.2 Student Roles and Responsibilities

4.2.1 Students are required to follow this Policy when processing any personal information as part of their studies/research.

4.2.2 Students are responsible for ensuring that they conform to this Policy and any Guidelines based on it when using personal information in undertaking their studies in and on behalf of ALC.

4.2.3 students are obliged to seek the approval of the Senate Research & Ethics Committee prior to conducting any research or academic activity that implies Personal Data and human subjects, in line with the regulations and guidelines provided by the Committee.

4.2.4 Students who have any queries with respect to Data Protection or these Guidelines should seek advice from the DPO

5. RIGHTS OF THE DATA SUBJECT/INDIVIDUAL

5.1 Individuals Rights

ALC will develop procedures and guidance to ensure that arrangements are made to provide for the rights available to Data Subjects under GDPR:

A. The right to be informed.
B. The right of access.
C. The right to rectification.
D. The right to erasure.
E. The right to restrict processing.
F. The right to data portability.
G. The right to object.
H. Rights in relation to automated decision making and profiling.
I. The right to data security and confidentiality

5.2 CONSENT

5.2.1 ALC will ensure that where consent is the legal basis for processing this consent meets the standards required.

5.2.2 Data Subject will take a positive action to provide consent that is explicit and freely given.

5.2.3 Consent will be separate from other terms and conditions.

5.2.4 Consent will not be a precondition of a service.

5.2.5 Consent will be specific and granular.

A. Data Subjects will be able to withdraw consent at any time and the process for withdrawing consent will be as easy as it was to give consent.
B. Evidence of consent will be retained.
C. Consent will be kept under review and renewed as required.

D. The institution will not use consent for core activities where there is an imbalance in the relationship between the institution and Data Subjects. Where this is the case an alternative condition for processing will be identified.
E. In recognition of the need to protect the rights of children the institution will take steps, when processing their personal data, to address their rights and the Data Protection Principles, in particular fairness.

5.2.2 The process for approval of research projects involving human participants will be implemented in line with the regulations developed in this regard by the Senate Research & Ethics Committee and will address the requirements of GDPR in relation to Data Subject rights and privacy.

6. DATA (INFORMATION) SECURITY

All personal data must be kept secure from unauthorized access. For computer-based information this would include the use of passwords, password protected screensavers, cryptographic-mechanisms, and physical forms of security including, portable media such as USB pens being locked away, etc.

Particular care must be taken when holding personal information on laptop computers. Personal information held on laptops should be deleted as soon as it is no longer required.

Personal data/information held on paper should be kept in locked cupboards and/or drawers unless it is being worked on. Personal data/information should not be downloaded to non-encrypted laptops/devices.

This is in line with the legal requirement to take appropriate security and organisational measures for the prevention of unauthorised access to, alteration of, disclosure of, accidental loss, and destruction of the data in his control; and to ensure that the measures provide a level of security appropriate to – (i)the harm that might result from unauthorised access to, alteration of, disclosure of, destruction of the data and its accidental loss; and (ii)the nature of the data concerned.

7. ACCOUNTABILITY AND GOVERNANCE

7.1 The controller shall implement appropriate technical and organisational measures such as pseudonymisation, data-protection principles, and data minimisation in order to effectively protect the rights of data subjects.

7.2 The controller shall implement proper technical measures to ensure that personal data which are essential for a specific purpose are processed. Obligation shall be based on the amount of data of collected personal data, extent of processing, period of storage and accessibility.

7.3 These measures will serve to ensure that by default, personal data are not accessed without the data subject's intervention.

7.4 The DPO will be accountable for ensuring GDPR compliance by the organisation, as well as evaluate and implement data protection policies.