DATA PROTECTION POLICY

Approving Authority	Council
Date of Approval	19th March 2026
Version #	2
Effective Date	20th March 2026
Date last reviewed	
Revision date(s)	
Responsible Officer	Data Protection Officer
Document URL	……

1. INTRODUCTION

1.1 This Data Protection Policy is the overarching policy for data protection and privacy for Botswana Open University (BOU).

1.2 BOU is committed to protecting the personal data of its employees, customers, partners, and stakeholders in compliance with the applicable data protection laws and regulations.

2. DEFINITIONS

2.1 **Automated decision-making and profiling** shall mean the making of decisions about an individual through automated processing, including the use of algorithms, without human intervention, and include the automated analysis of personal data to evaluate, analyse, or predict an individual's characteristics, behaviour, or outcomes.

2.2 **BOU or University** shall mean the Botswana Open University.

2.3 **Child** shall mean any person under the age of 18 years.

2.4 **Commission** shall mean the Information and Data Protection Commission established under section 6 of the Data Protection Act (DPA).

2.5 **Data Subject** shall mean a natural person who is the subject of personal data.

2.6 **DPA** shall mean the Data Protection Act No.18 of 2024.

2.7 **Data Protection Impact Assessment** shall mean a systematic process required to evaluate the potential risks to individuals' personal data when starting a new project.

2.8 **DPO** shall mean the Data Protection Officer appointed in terms of

Section 69 of the DPA.

2.9 **EMT** shall mean the Executive Management Team of Botswana Open University.

2.10 **Personal Data, Personal Information, or Personally Identifiable Information** shall mean any information relating to an identifiable person. It includes details that can directly or indirectly identify an individual, such as a name, identification number, or location data.

2.11 **Personal Data Breach** shall mean any security incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored, or otherwise processed.

2.12 **Pseudonymised Data** shall mean data that can no longer be attributable to a specific data subject without the use of additional information.

2.13 **Processing of Personal Data** shall mean any operation, or a set of operations performed on personal data which may occur by automatic means. It includes collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, dissemination, erasure, or destruction.

3. PURPOSE

3.1 The purpose of the Data Protection Policy is to ensure compliance with the Data Protection Act (2024) and all other relevant legislation.

3.2 BOU recognises data protection as a fundamental right and embraces the principles of data protection by design and by default.

4. SCOPE

4.1 This Policy applies to all employees, including temporary staff, contractors, and third parties who handle personal data on behalf of the University.

4.2 The Policy covers all personal data collected, processed, stored, or shared by the University, whether in electronic or physical form.

5. PRINCIPLES

5.1 The University will:

5.1.1 Establish and maintain underpinning policies to ensure compliance with the Data Protection Act 2024, the General Data Protection Regulations, and other relevant legislation.

5.1.2 Establish and maintain policies for the controlled and appropriate sharing of service user and staff information with other agencies, taking into account all relevant legislation and data subject's consent.

5.1.3 Where consent is required for the processing of personal data, ensure that informed and explicit consent is obtained and documented in clear, accessible language and in an appropriate format, attached at Appendix A.

5.1.4 Where the data subject wishes to withdraw their consent, ensure that it is easy to withdraw consent at any time through procedures that have been outlined to them, provided in the Record Keeping Policy: Withdrawal of Consent procedures.

5.1.5 Undertake annual audits of BOU's compliance with legal requirements.

5.2 The University shall uphold the rights of data subjects outlined in the

Data Protection Act;

5.2.1 The right to be informed.

5.2.2 The right of access.

5.2.3 The right to rectification

5.2.4 The right to erasure.

5.2.5 The right to restrict processing.

5.2.6 The right to data portability.

5.2.7 The right to object.

5.2.8 Rights in relation to automated decision making and profiling.

5.3 BOU acknowledges accountability in ensuring that personal data shall be:

5.3.1 Processed only for legitimate business purposes, including but not limited to employee administration, student services, marketing, and regulatory compliance.

5.3.2 Processed lawfully, fairly, and transparently in accordance with applicable laws.

5.3.3 Relevant, accurate, and limited to what is necessary for the intended purpose.

5.3.4 Audited for accuracy with steps taken to ensure that inaccurate data is erased or rectified without delay.

5.3.5 Stored securely using appropriate technical and organisational measures.

5.3.6 Retained only for as long as necessary to fulfil the purposes for which it was collected, unless otherwise required by law. When data is no longer needed, it is securely deleted or anonymised.

6. DATA PROTECTION BY DESIGN AND BY DEFAULT

6.1 BOU shall implement appropriate organisational and technical measures to uphold the principles outlined above by integrating necessary safeguards to any data processing to meet regulatory requirements and to protect individuals' data rights. This implementation will consider the nature, scope, purpose, and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

6.2 BOU shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

6.3 All new systems used for data processing will have data protection built in from the beginning of the system change.

6.4 All existing data processing shall be recorded on the Record of Processing Activities. Each process shall be risk assessed and reviewed annually.

6.5 BOU shall ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

6.6 In all processing of personal data, BOU will use the least amount of identifiable data necessary to complete the work it is required for. BOU will only keep information for as long as it is required for the purposes of processing or for any other legal requirement to retain it, and in accordance with the BOU Retention and Disposal Schedule.

6.7 Where possible, pseudonymised data shall be used to protect the privacy and confidentiality of BOU staff, students, and Clientele.

6.8 Data Security Measures

The University shall implement appropriate security measures to prevent unauthorised access, disclosure, alteration, or destruction of personal data. Access to personal data is restricted to authorised personnel only. Employees and contractors handling personal data shall receive regular training on data protection practices.

6.9 Data Transfers

Personal data may be transferred to third parties either locally or to cross-border locations only if adequate data protection safeguards are in place. The University shall ensure compliance with applicable data transfer regulations, including standard contractual clauses or other approved mechanisms. When transferring personal data outside Botswana, the University shall retain a complete copy within Botswana, kept up-to-date and synchronised.

6.10 Data Breach Management

In the event of a personal data breach, the University shall:

6.10.1 Take immediate action to contain and assess the breach.

6.10.2 Ensure the Commission is notified within the prescribed 72-hour timeframe.

6.10.3 Prepare a detailed incident report and implement corrective measures immediately.

6.10.4 Keep a record of all personal data breaches.

6.10.5 Where the personal breach is likely to result in a high risk to the rights and freedoms of data subjects, the University shall communicate the breach to the data subject without undue delay.

7. DATA GOVERNANCE ROLES AND RESPONSIBILITIES

7.1 The University Council

The Council has overall responsibility and oversight of data protection and sets the tone from the top. It approves the Data Protection Policy. Regular updates from the EMT informs the Council about the University's performance regarding data protection.

7.2 The Vice Chancellor and the EMT

7.2.1 The ultimate responsibility for data protection compliance, cultivating a compliance culture within the University, and ensuring that adequate resources are in place lies in the Executive Team. EMT is responsible for ensuring the organisation adheres to relevant data protection and privacy laws and industry standards.

7.2.2 EMT shall ensure that all Employees and 3rd Party Service Providers are aware of, briefed, and adhere to the requirements of this Policy.

7.2.3 EMT has a responsibility to ensure that objectives and plans for compliance with DPA are established and reviewed annually, or as scheduled during the Management Review meetings, and that the roles and responsibilities for the processing of the personal data and information security are defined.

7.2.4 Each Executive member has a responsibility to ensure that persons working under their control will protect information in accordance with the University policies.

7.2.5 Each Executive member shall take appropriate action against any Employees and third-party service providers under their care found to have contravened this Policy.

7.3 BOU Staff

All Employees are required to comply with this policy, and non-compliance may result in disciplinary action.

7.4 Data Protection Officer

7.4.1 In line with legislation, the University shall recruit a Data Protection Officer (DPO) who reports to the Vice Chancellor. The DPO shall ensure compliance with data protection laws and regulations, develop and implements the Data Protection Policy and procedures.

7.4.2 In addition, the DPO advises and reviews Data Protection Impact Assessments (DPIA) and maintains records of processing activities. Undertake and commission data protection audits, and handles all queries and complaints from clients and staff, and serve as the point of contact for the data protection regulator.

8. PROCESSING OF CHILDREN'S PERSONAL DATA

When the University processes the personal data of a child, it shall obtain consent from a parent or any person with parental responsibilities in accordance with the Children's Act. Where the child has reached the age of sixteen (16) years, the child may provide consent in the manner prescribed by law. Where appropriate, and taking into account available technological measures, the University shall take reasonable steps to confirm that consent has been provided by both the child and the parent or person exercising parental responsibilities.

9. AUTOMATED DECISION-MAKING AND PROFILING

Botswana Open University shall not make decisions that significantly affect a person based solely on automated processing or profiling, unless permitted by law. Where automated decision-making is used, the University shall ensure the process is lawful, fair, transparent, and supported by appropriate safeguards. Data subjects shall be informed about such processing and have the right to human intervention**.**

10. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

The University shall conduct Data Protection Impact Assessments (DPIAs) where personal data processing is likely to result in a high risk to the rights and freedoms of data subjects. In particular, the University shall undertake a DPIA in circumstances that include, but are not limited to:

a) the introduction or use of new or innovative technologies;

b) automated decision-making or profiling activities;

c) large-scale processing of special category personal data; and

d) large-scale, systematic monitoring of publicly accessible areas.

11. UNDERPINNING POLICIES, PROCEDURES AND CONTRACTS

This Policy is underpinned by the following:

11.1 General Conditions of Service – It guides on the standard of behaviour and conduct the University expects of its employees, including matters necessary for the protection of data, such as confidentiality, removal, and erasure of documents.

11.2 Records Management Policy – This details transparency procedures, the management of records from creation to disposal (inclusive of retention and disposal procedures) Information handling procedures, procedures for subject access requests, right to erasure, right to restrict processing, right to object, and withdrawal of consent to share.

11.3 Information Technology Policies (ICT Policy Framework, Change Management Policy, Backup Policy, Systems Access Policy, Network Security Policy, Password Policy, Bring Your Own Device Policy, Acceptable Use Policy) – Outline procedures for ensuring the security of data, including the reporting of any data security breach.

11.4 Business Continuity Plan – It outlines the procedures in the event of a security failure or disaster affecting digital systems or mass loss of hardcopy information necessary to the day-to-day running of our organisation.

11.5 BOU Risk Management Framework

11.6 BOU Compliance Policy

11.7 Data Transfer Agreement

11.8 Data Sharing Agreement

12. REVIEW

This Policy shall be reviewed every three years or earlier as necessary.