Botho University
Data Protection Policy

1 Introduction

1.1 Botho University gathers and processes Personal Data in respect of its students, staff, and other individuals in order to carry out its functions, to provide its services and to meet legal and regulatory obligations.

1.2 The University is committed to protecting the privacy of all individuals by ensuring the fair, responsible and transparent use of all Personal Data that it holds. The University aims to comply with the current legislation in place in the various countries that the University has operations. In Botswana, the University will comply with the Data Protection Act, 2024.

1.3 This Policy and the Data Protection Code of Practice guides the University to comply with legislation and seeks to ensure that all Policy users are clear about how Personal Data must be processed to comply with Data Protection Law and best practice.

2 Scope

2.1 This Policy applies to all University staff and students, and any other individual processing Personal Data held by or on behalf of the University.

2.2 This Policy applies to all recorded information which relates to identified or identifiable individuals, irrespective of the format in which that information is held and regardless of the location where Personal Data is stored e.g., it applies equally to Personal Data stored on an employee device and student's own device particularly with respect to student coursework or research.

2.3 This Policy does not apply to information processed by any other entities which are located on University premises but are not owned or managed by the University and which have separate legal identities.

3 Guidance and related policies

3.1 This Policy is accompanied by the Data Protection Code of Practice which is to be followed by all those to whom this policy applies in order to achieve the University's policy objectives. Reference should also be made to the University's Information Governance and Management Policy and the Data Breach Management Policy. Copies of the Data Protection Code of Practice and related policies are available here.

4 Definitions

4.1 All definitions in this policy have the same meaning as under the Botswana Data Protection Act, 2024

Data Controller: a person or public authority which alone or with others determines the purposes and means of the processing of personal data (Botho University)
Data Processor: a person who processes personal data on behalf of the data controller (Staff)
Data Subject: a natural person whose data is being processed
Data Protection Officer: a person designated for Data Protection Act action and liaison
Consent: any freely given, specific, informed and unambiguous indication of the data subject wishes by which he or she by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
Personal Data: any information relating to an identified or identifiable natural person or data subject. An identifiable natural person is one who can be identified directly or indirectly by reference to an identifier such as a name, an identification number, location data and 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 Data Breach: a breach of security leading to the accidental or unlawful distraction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored, or otherwise processed.

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 and includes collection, recording, organising, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available alignment or combination, restriction, erasure or destruction

Pseudonymisation: processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information.

Recipient: a natural or legal person or a public authority to which personal data is disclosed, whether a third party or not.

Restriction of processing: the marking of stored personal data with the aim of limiting their processing in the future.

Sensitive Personal Data: revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership or 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 sex life or sexual orientation and includes personal data relating to a data subject which reveals commission or any alleged commission of any offence by him or her.

Third Party: a natural or legal person or public authority other than the data subject, data controller, data processor and persons who under the direct authority of the data controller or data processor are authorised to process personal data.

4.2 The University as Data Controller has a corporate responsibility to process Personal Data with due regard to the rights and freedoms of individuals, and to comply with the requirements of Data Protection Law.

4.3 The legislation requires that a Data Protection Officer (DPO) is appointed. It is the role of the DPO to assist the University in monitoring internal compliance, inform and advise on data protection obligations and act as a contact point for data subjects and the Information and Data Protection Commissioner's Office. The DPO also helps demonstrate compliance in accordance with the enhanced focus on accountability.

5 Data Protection Principles

5.1 Any individual processing Personal Data should adhere to the principles of lawfulness, fairness, and transparency, which are set out in Data Protection Act, 2024 Part IV.

5.2 The University as the Data Controller shall be responsible for demonstrating compliance with the above stated principles and will implement appropriate technical and organisational measures to ensure compliance.

5.3 The Data Protection Code of Practice details how these Principles are to be applied in practice to University activities.

6 Lawful basis for processing

6.1 The first data protection principle stipulates that Personal Data must be processed lawfully. The University shall ensure that a lawful basis for processing Personal Data and Sensitive Personal Data is identified for each processing activity. The data processor must confirm and document lawful basis which apply to its processing activity prior to the processing activity being carried out.

6.2 Lawful basis for processing Personal Data

6.2.1 Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract with the data subject.

6.2.2 Processing is necessary to comply with a legal obligation.

6.2.3 Processing is necessary to protect the vital interests of a data subject or another person.

6.2.4 Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

6.2.5 Processing is necessary for the purposes of legitimate interests pursued by the Data Controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

6.3 The Botswana Data Protection Act, 2024 Part VI specifically states provisions for the lawful processing of Sensitive Personal Data and Part VII states provisions related to specific processing situations. In respect of these sections of the law the University will adhere to the stated requirements.

6.4 Where the University is processing Personal Data that relates to an actual or alleged criminal offence, the University shall abide by the provisions of Section 32 of the Botswana Data Protection Act, 2024.

7 Consent

7.1 Where the University is relying on consent to lawfully process Personal Data, the consent must be specific, informed and freely given.

7.2 The University will clearly inform data subjects how they can withdraw their consent.

8 Processing of Child Personal Data

8.1 Whilst most of the University's activities involve the processing of adult Personal Data, it is recognised that in some circumstances the University will process Personal Data belonging to children.

8.2 When processing a child's personal data, the University shall seek consent and authorisation by a parent or person who has parental duties over the child in terms of the Children's Act. Where the child is 16 years of age, such child may give consent in such a manner as may be prescribed. The University shall, where appropriate and considering available technology, make reasonable efforts to verify that consent is given jointly by the child and the parent or person who has parental duties over the child.

9 Rights of Individuals

9.1 The University will comply with the rights given to individuals under the Botswana Data Protection Act, 2024.

9.2 Individuals who wish to exercise any of their rights as per the BDPA shall contact the University's Data Protection Officer through the Office of Vice-Chancellor: dpo@bothouniversity.ac.bw ; or send a request in writing to the Office of the Vice-Chancellor.

9.3 The University will make all efforts to ensure that response times to any requests as above are within the limits set by the BDPA. Normally the processing of a request would not be charged unless the DPO believes the request is unreasonable and excessive in nature.

9.4 Members of staff who receive a request to exercise any of the rights as per the Botswana Data Protection Act, 2024 must contact the Data Protection Officer or any member of the Office of Vice-Chancellor without delay so that the request can be processed within the prescribed time for a response.

10 Data Protection Impact Assessments

10.1 The University is required to ensure that it follows suitable procedures to ensure privacy of data subjects when processing personal data. This requires the University to have the necessary technical and organisational measures to ensure that by default, only personal data which is necessary for any particular purpose is processed.

10.2 The University must also carry out Data Privacy Impact Assessments (DPIAs) in respect of high-risk processing. The University will make efforts to carry out a DPIA in the following circumstances:

10.2.1 When using new technologies

10.2.2 When using automated processing or profiling

10.2.3 Large scale processing, in particular, of special category data

10.2.4 Large scale systematic monitoring of a publicly accessible area

11 Responsibilities of Staff

11.1 All staff must comply with the requirements of this Policy.

11.2 Staff may only process Personal Data to the extent to which they have been specifically authorised by the University or are generally authorised as part of their role within the University.

11.3 Staff are responsible for ensuring that any Personal Data processed in the course of their employment is managed securely. Specifically, individuals are responsible for ensuring that Personal Data in their possession is not left unsecure, for example in meeting rooms, public spaces, open plan environments or mobile devices, without adequate protection.

11.4 Staff must ensure that existing and new business processes, activities and systems (e.g. IT software) are compliant with the requirements of the Data Protection Act, this Policy and Data Protection Code of Practice. Furthermore the Data Protection Officer must be made aware of any significant changes to the processing of Personal Data. Specific advice can be provided by the DPO as required.

11.5 Staff must undertake DPIAs, with support from the DPO in the circumstances referred to above, prior to commencing any high-risk processing activity, in accordance with the Data Protection Code of Practice and any University guidance on DPIAs.

11.6 Staff must ensure that privacy information is communicated to Data Subjects at the point of collection of Personal Data.

11.7 Academic staff are responsible for ensuring that their students are fully informed about their responsibilities under the Act with regard to any specific coursework or research which involves the gathering or processing of Personal Data. Academic staff authorising the processing of Personal Data by students for the purpose of coursework or research are responsible for the monitoring of that processing.

11.8 Research Ethics Committees at all levels within the University will take appropriate measures to ensure that the research activities of students and staff are compliant with data protection requirements.

12 Responsibilities of Students

12.1 In connection with their academic studies/research, all University students have the following responsibilities:

12.1.1 to notify an appropriate member of staff, usually their tutor, if they intend to process information about identifiable individuals as part of their academic studies/research.

12.1.2 to only process Personal Data for use in academic studies/research which has been expressly authorised by a member of staff or the appropriate Research Ethics Committee.

12.1.3 to comply with any regulations or requirements implemented by the University or by a member of University staff in order to facilitate compliance with Data Protection Law;

12.1.4 to have reference and to adhere to the University Policy, Procedures and Guidelines for Research Ethics.

12.2 In relation to any activities not specifically authorised by the University, students processing Personal Data are responsible for their own compliance with Data Protection Law.

13 Reporting a Personal Data Breach

13.1 It is a requirement of Botswana Data Protection Act, 2024 that any personal data breaches are reported to the authorities where there is a serious risk to the rights and freedoms of a Data Subject. The University shall put in place the required processes to report any breaches. Reference is made to the Data Breach Management Policy.

14 Sharing Personal Data

14.1 The University may legitimately share personal information either within the University, or with an external third party, provided it has identified an appropriate lawful basis to do so.

14.2 Where systematic data sharing is taking place with a separate data controller, the University may consider creating a Data Sharing Agreement (DSA) to document this process. Data Sharing Agreements must be approved by the University's DPO.

14.3 Ad-hoc data sharing, for example to assist in the prevention or detection of crime, is permitted where there is an identified lawful basis to do so. Instances of ad-hoc disclosures of personal data should be documented for accountability purposes.

15 Transfers of Personal Data outside Botswana

15.1 Transfers of data outside Botswana are guided by the Botswana Data Protection Act, 2024, and data transfers are only permitted in the following situations:

15.1.1 The country receiving the Personal Data is considered to provide an adequate level of protection;

15.1.2 Appropriate safeguards are in place such as binding corporate rules or standard contractual clauses (for example, use of the International Data Transfer Agreement (IDTA));

15.1.3 The data subject has provided explicit consent to the proposed transfer;

15.1.4 The transfer is necessary for one of the reasons set out in the Botswana Data Protection Act, 2024 including:

15.1.4.1 The performance of a contract;

15.1.4.2 Reasons of public interest;

15.1.4.3 For the establishment or defence of legal claims;

15.1.4.4 In the Vital Interests of a Data Subject.

15.2 Where transfers are being made out of Botswana, advice should be sought from the Office of the Vice-Chancellor to ensure compliance.

16 Training and Audit

16.1 The University will ensure that all staff receive appropriate training to enable them to comply with this Policy and Data Protection Law.

16.2 Data Protection training is mandatory for all employees.

16.3 Any individual who does not think they are sufficiently aware of Data Protection Law must contact the Human Resources Department or the Office of the Vice-Chancellor to arrange additional training.

16.4 The University will regularly test systems and processes to monitor compliance.

17 Policy Enforcement

17.1 Failure to follow this Policy and the Data Protection Code of Practice may result in disciplinary action.