HOLMES UNIVERSITY BOTSWANA

Privacy and Data Protection Policy

Policy Overview

Summary	The aims of this policy are to: 1. Set out the expectations, procedures and protocols in relation to how personal data is received, managed and processed 2. Assist to ensure our adherence and compliance to privacy and data protection legislation. 3. Minimise risk relevant in relation to personal data breaches and other breaches of data protection legislation.		
Policy Owner	Director of Risk and Compliance as Data Protection Officer (DPO)		
Policy Sponsor	Board of Directors, Chaired by the CEO		
Policy applies to	All staff		
Equality impact assessment completed	This policy, and the privacy and data protection legislative framework, acknowledge that personal data relating to individuals with protected characteristics needs to be carefully managed and controlled. This data, considered to be Special Category Personal Data, is likely to be more sensitive, or private, and therefore likely to cause more damage or distress if compromised. It is therefore given additional protection in data protection legislation and in this policy.		
Relevant Legislation and Policies	The Data Protection Act – Act No. 18 of 2024		
Version	1.1		
Approved by	Board of Directors	**Approval date**	01 June 2026
Date of implementation	1 June 2026	**Date of next formal review**	3 years following approval date.

1. INTRODUCTION

1.1 Holmes Institute Botswana (HIB) is committed to protecting the privacy and security of personal data belonging to our staff, students, and other stakeholders including research subjects.

1.2 This policy sets out the Policy Statement of HIB relevant to the protection of personal data. It further highlights the roles and responsibilities of HIB and its officers regarding the collection, processing, security of and access to personal data. Further, this policy details the framework for investigating and preventing data breaches, as well as governance and training arrangements to ensure ongoing compliance to this policy.

1.3 In adopting this policy, HIB desires to mitigate risk relevant to personal data breaches and other breaches of data protection legislation.

1.4 The Data Protection Act, Act No. 18 of 2024, provides for the continuation of the Information and Data Protection Commission as Botswana's data protection regulator. HIB will engage with and/or notify the Information and Data Protection Commission where required by applicable data protection legislation, including in relation to data protection complaints, reportable data breaches, audits, investigations or regulatory requests.

2. POLICY STATEMENT

2.1 This policy aims to:

2.1.1 Set out the expectations, procedures and protocols in relation to how personal data is received, managed and processed at HIB.

2.1.2 Assist to ensure HIB's adherence and compliance to privacy and data protection legislation.

2.1.3 Minimise risk relevant to personal data breaches and other breaches of data protection legislation.

2.2 To achieve these aims and with reference to relevant data protection principles and data subject rights, HIB undertakes to:

- Make privacy and data protection a core part of business operational activities;
- Provide staff training in relation to this policy and the management of personal data;
- Ensure that the collection and use of personal data is only done for specific and legitimate purposes;
- Process personal data in a lawful and transparent manner;

- Disclose to Data Subjects how their personal information is to be used (by way of a privacy notice at the transmission point of personal data);
- Only maintain personal data that is accurate and up to date and delete data that is inaccurate or out of date;
- Only retain personal data for as long as it is necessary to do so (with the exclusion of retention for public interest or statistical purposes);
- Prioritise keeping personal data confidential and secure;
- Not share personal data with third parties unless adequate standards of data protection can be guaranteed by that third party;
- Not share personal data with third parties unless this is disclosed to and agreed to by data subjects;
- Incorporate data protection measures and standards into HIB's corporate governance structure through reporting to the Board on adherence to this policy and to relevant legislation.

2.3 This policy is to be read in conjunction with HIB's Privacy Notice.

3. SCOPE OF POLICY

3.1. This policy applies to all HIB activities and processes in which personal data is used, regardless of whether it is in a digital or hard copy format.

3.2. This policy applies to HIB staff and students and to others acting for or on behalf of HIB who are granted access to our information infrastructure.

4. KEY DEFINITIONS

- **Data Controller:** A person, public authority, agency or other body that determines the purposes and means of processing personal data. HIB is the Data Controller for the purposes of this policy. A Data Controller is responsible for a Data Processor's use of information and must take steps to ensure that a Data Processor is able to protect and adhere to legislation regarding personal data before providing it to the Data Processor.
- **Data Processor:** A person, public authority, agency or other body that processes personal data on behalf of the Data Controller. This could be an agent or a contractor.

- **Data Protection Officer (DPO):** The person responsible for informing and overseeing that HIB is meeting its data protection obligations and for monitoring HIB's compliance with them. At HIB, the DPO is the Director of Risk and Compliance.

- **Data Subject:** The identified or identifiable living individual to whom personal data relates.

- **Personal Data**: Any information relating to a person (Data Subject) who can be identified, directly or indirectly, through 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 person. HIB processes personal data relating to a number of categories of Data Subject, including employees, students, applicants, business contacts, visitors, suppliers and contractors.

- **Data Breach (DB):** A security incident that has affected the confidentiality, integrity or availability of personal data. A data breach occurs whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; accessed or passed on without proper authorisation; or is made unavailable and this unavailability has a significant negative effect on individuals.

- **Information and Data Protection Commission**: Botswana's data protection regulator under the Data Protection Act, Act No. 18 of 2024, responsible for oversight and enforcement of Botswana's data protection framework.

- **Processing:** In relation to personal data, Processing means almost anything HIB might do with personal data or sets of personal data (whether or not by automated means) such as collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction.

- **Special Category Personal Data:** Personal data that is likely to be more sensitive, or private, and therefore likely to cause more damage or distress if compromised. It is therefore given additional protection in data protection legislation. The categories are:

    - personal data revealing racial or ethnic origin;
    - personal data revealing political opinions;
    - personal data revealing religious or philosophical beliefs;
    - personal data revealing trade union membership;
    - genetic data;
    - biometric data (where used for identification purposes);
    - data concerning health;
    - data concerning a person's sex life and
    - data concerning a person's sexual orientation.

5. RESPONSBILITIES OF GROUPS/INDIVIDUALS WITHIN THE DATA CONTROLLER

5.1 The **Board** has overall oversight of this policy and has ultimate responsibility for ensuring that there is a current Privacy and Data Protection Policy in place and that relevant systems are set up within the organisation to protect privacy and data in accordance with this policy.

5.2 The **Director of Risk and Compliance** is responsible for advising the Board about HIB's data protection obligations under this policy and pursuant to legislation; training HIB's staff about this policy; monitoring compliance with and ensuring enhancements to this policy; processing subject access requests at HIB; investigating data breaches and reporting these to the Board and other appropriate individuals/entities; and coordinating with external bodies relevant to data protection.

5.3 The **HIB SMT** is responsible for ensuring data protection compliance within their departments; liaising with the DPO to ensure that relevant staff are up to date with training; ensuring that agents, contractors and other Data Processor under their control or influence are up to date with this policy and are adhering to it.

5.4 All **HIB staff** are responsible for ensuring that they comply with this policy and conduct training relevant to this policy on a regular basis (within two years of their last training). All HIB staff are also responsible for ensuring that personal data is kept securely; not disclosed to any unauthorised third parties; kept in accordance with data retention schedules. All HIB staff are required to be aware that if there are subject access requests or complaints, that these are to be referred to the Director of Risk and Compliance within 24 hours of becoming aware of such a request or complaint being made. Finally, all staff are required to report any suspected breaches of this policy to their line manager or directly to the DPO.

5.5 **Students** will be made aware of the Privacy Notice and Privacy and Data Protection Policy so that they can understand how their data is collected and managed, and know who to escalate a suspected data breach to. Through awareness of this policy, students should be aware of their own need to respect the privacy and personal data of staff, students, industry and wider community.

5.6 **Students** have an obligation to ensure that their data is up to date with HIB.

6. PRIVACY NOTICE

6.1 HIB's Privacy Notice (hyperlink) is to be read in conjunction with this policy and a link to this policy can be found within this policy or on HIB's website.

6.2 The Privacy Notice makes staff, students, and other stakeholders aware of HIB's commitment to privacy and data protection, details more precisely the type of data that HIB will collect, and explains how HIB will store, process and use personal data.

6.3 HIB's Privacy Notice may be updated from time to time. The most current version will be published on HIB's website. Past versions of this Privacy Policy may be available by request to the DPO.

7. DATA PROTECTION IMPACT ASSESSMENT

7.1 As part of HIB's commitment to enhance its privacy and data protection and to meet individuals' ongoing and changing privacy expectations, HIB will use Data Protection Impact Assessment (DPIAs) from time to time to help identify and reduce data protection risks relating to our processes and consider any data sharing arrangements HIB has in place with data processors.

7.2 The outcome of any such DPIA may result in a change of this policy and/or a change in the Privacy Notice and/or a change in operations.

7.3 As a Data Controller, HIB ultimately remains responsible for the use of information it has passed to any Data Processor. It therefore must ensure that a Data Processor is capable of protecting personal data before providing it them.

7.4 A DPIA will be undertaken by HIB's DPO from time to time.

7.5 A template for DPIAs is available at **Appendix A**.

7.6 Any DPIA undertaken will be maintained by the DPO by way of a register, and any completed DPIAs *may* be made available to appropriate authorities on request.

8. SHARING DATA WITH THIRD PARTIES

<u>With Data Controllers</u>

8.1 HIB will, where it is required to do so, put in place a data sharing agreement with third party Data Controllers.

8.2 A data sharing agreement will include details about:

- 8.2.1 the parties' roles;
- 8.2.2 the purpose of the data sharing;
- 8.2.3 what is going to happen to the data at each stage;
- 8.2.4 ongoing checks and balances to ensure information and processes remain current.

8.3 Any third party intending to make a data sharing agreement with HIB should first speak to the DPO to ensure that an appropriate template is used.

8.4 A register of Data Sharing Agreements will be maintained by the DPO and Data Sharing Agreements will be made available to appropriate authorities on request.

<u>With Data Processors</u>

8.5 HIB will, where it is required to do so, put in place a data sharing agreement with third party Data Processors.

8.6 Data sharing agreements with Data Processors ought to include the following details relating to the data processing:

- subject matter of the processing;
- duration of the processing;
- nature and purpose of the processing;
- type of personal data involved;
- categories of data subject; and
- controller's obligations and rights

8.7 The DPO will maintain a register of all current processor contracts, which will be updated when processors change.

9. DATA BREACHES

9.1 HIB will use its best endeavours to ensure that personal data is kept secure. As part of exercising its best endeavours, HIB will implement appropriate technical measures (e.g. encryption, access control, password protection etc.) to mitigate the risk of personal data beaches. In addition to this, all staff will be made aware of and trained in data protection protocols and procedures as to avoid the unauthorised or unlawful processing and the accidental loss, destruction or damage of personal information.

9.2 Should a personal data breach occur, HIB will manage the incident as follows:

9.2.1 All suspected and actual data breaches will be reported to the DPO as soon as possible. HIB staff may escalate an actual or suspected breach via their supervisor and students can escalate any suspected breach to a Student Support Officer. Reports should be made as a matter of urgency by the DPO. A Data Breach Report Template is at **Appendix B**, with some examples within that Template as to what may constitute a data breach.

9.2.2 In the first instance, the DPO with the assistance of relevant staff members, will control and contain any data breaches to recover data, prevent further breaches and minimise harm.

9.2.3 The DPO will then:

9.2.3.1 assess the risks associated with data breach to determine the next steps in terms of containing the breach;

9.2.3.2 notify relevant parties, including the Information and Data Protection Commission where required by applicable data protection legislation (taking into account legal, regulatory and contractual notification requirements as well as the need to notify datasubjects who may have been affected);

9.2.3.3 take steps to prevent further breaches occurring by implementing specific and systemic improvements; consider whether any staff disciplinary or student misconductprocedures need to be instigated where there is evidence of

non- compliance with this policy; and,

9.2.3.4 ensure records of the data breach and HIB's response are maintained and that the effectiveness of HIB's response is reviewed by the Board.

10. SUBJECT ACCESS REQUESTS

10.1 Data Subjects are entitled to ask HIB to provide them with a copy of any information that HIB holds about them. The right of access, commonly referred to as "subject access" gives individuals the right to obtain a copy of all personal data that HIB holds about them.

10.2 Subject Access Requests (SARs) can be made to the DPO but can be made via other communication mediums as well (such as by email, letter and over the phone).

10.3 The DPO will process requests in accordance with the legislation.

10.4 Staff are required to assist the DPO in providing relevant information as a priority.

10.5 In certain circumstances, HIB may be entitled to charge an administration fee to the person making the SAR, which may take into account factors such as processing the information, the cost of locating the information, retrieving and extracting the costs of communicating and providing copies of the information etc. The DPO will determine whether a feewill be charged and what a reasonable fee will be.

10.6 If anyone (for example, the Police or the spouse or parent of a data subject) requests access to personal data relating to another person, staff must first check with the DPO before making a disclosure.

10.7 Further information about data subject rights is accessible via HIB's Privacy Policy.

11. GOVERNANCE

11.1 HIB's governance in relation to privacy and data protection is evidenced by:

11.1.1 The appointment of the Director of Risk and Compliance as the DPO;

11.1.2 The DPO providing reports to the Board on matters relevant to this policy.

11.1.3 The DPO being responsible for providing a Data Breach Report to the Board on any suspected or actual data breach and for retaining a report of any such suspected or actual breach for a period of 2 years;

11.1.4 The DPO's disclosure to relevant authorities, including the Information and Data Protection Commission where required, of any significant breaches of privacy or data protection

11.1.5 HIB adhering generally to the principles of privacy and data protection and making the protection of data part of its ethos and operations function;

11.1.6 HIB will publishing and keep updated a Privacy Notice on its website to inform Data Subjects, as well as other stakeholders about how HIB collects, manages and processes personal data.

12. TRAINING

12.1 HIB ensures that staff are up to date with current privacy and personal data protection legislation. This is done at staff onboarding and then with an ongoing refresher training at least once every two years.

12.2 The training process and a register of people within the organisation trained is to

be maintained by the DPO.

12.3 This policy will be disseminated to all staff via the HIB website. Should staff, students or other stakeholders have queries relevant to this policy or about privacy or data protection generally, they may contact the DPO.

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the Information and Data Protection Commission, where required, before proceeding
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

APPENDIX B: Data Breach Report

Data Security Incident Report Form			
Date incident occurred:		Date incident reported:	
Location of incident:			
Does the breach involve personal data?	Yes ☐ No ☐		
Type of data breach: *(Indicate what form the data was in when the incident occurred)*	☐ Digital – e.g. Hacking, Virus, Ransomware, file corruption etc. ☐ Electronics – e.g. lost laptop, phone, USB device ☐ Verbal – e.g. wrong information given over the phone ☐ Paper – e.g. lost or misplaced file etc.		
Details of incident: *(State facts only and **not** opinions. Include details of staff involved and any contributing factors)*			
Reporter details			

Name:		Job title:	
Signature:			
To be completed by DPO			
Incident details *(if more space is required please keep with this initial form).* This should include • Type and number of individuals involved • Types of data • Number of records concerned			
Likely consequences of the breach. *(Especially note if there is potential risk to the rights and freedoms of an individual.)*			
Action taken *(if more space is required please keep with this initial form).* Describe the measures taken or which will be taken to deal with and mitigate the attack.			
Have relevant authorities been informed? Only in the instance that an individual's rights or freedoms are likely to be at risk.	Yes ☐ No ☐ N/A ☐		
Has the data subject been informed? Only in the instance that their rights or freedoms are likely to be at risk.	Yes ☐ No ☐ N/A ☐		
DPO Name:			
Signature:		Date:	