Botho University
Data Protection Code of Practice

BOTHO UNIVERSITY
VIBRANCE • INNOVATION • IMPACT

Introduction

This Code of Practice accompanies the University's Data Protection Policy and provides practical guidance around how to implement and adhere to the Data Protection Policy. Definitions in this Code of Practice are the same as in the Data Protection Policy and reflect definitions in the Botswana Data Protection Act 2024.

1 General requirements when processing Personal Data

1.1 This section applies to any processing of Personal Data, including collection, use, storage, disclosure and disposal. Personal Data must be processed in line with the Data Protection principles. This section describes what this means in practical terms.

1.2 Personal Data shall be processed lawfully, fairly and in a transparent manner. This means that staff will:

1.2.1 identify an appropriate lawful basis (refer to the Data Protection Policy for a list of lawful bases) for any processing;

1.2.2 provide privacy notices that clearly define the nature and purpose of processing and state the lawful basis for processing so that Data Subjects are fully aware what, how and why their data is being processed;

1.2.3 handle Personal Data only in ways defined by those notices, treating all Data Subjects equally;

1.2.4 not process Personal Data in ways which would have unjustified adverse effects on the individuals concerned;

1.2.5 not do anything unlawful with Personal Data.

1.3 Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means that staff will:

1.3.1 document the lawful basis for processing in the University's Record of Processing Activity (ROPA) as per the ROPA template;

1.3.2 not further process Personal Data that has been obtained for a specific purpose for any incompatible purpose unless a further lawful basis has been identified. Each non-compatible, further processing activity will require a lawful basis before proceeding. If further processing is compatible with the original purpose and is identified in an existing privacy notice which has been circulated to subjects, no further action will be required.

1.4 Personal Data shall be adequate, relevant and limited to what is necessary in relation to the processing purpose. This means that staff will:

1.4.1 collect only enough Personal Data to satisfy the specified purpose;

1.4.2 review datasets on an ongoing basis to use to ensure that fields of data that are not required, are removed;

1.4.3 Ensure that when Personal Data is no longer required for specified purposes it is deleted or anonymised in accordance with the University's Information Governance and Management Policy and the applicable data/record Retention schedule.

1.5 Personal Data shall be accurate and, where necessary, kept up to date. This means that staff will:

1.5.1 take reasonable measures to ensure that Personal Data is accurate at the point of collection; this is of particular importance when data is obtained from any source other than the subject themselves, as there is a higher likelihood that errors may have been made;

1.5.2 take reasonable steps to ensure data is up to date, such as periodically requiring data subjects to verify their contact details; and

1.5.3 Act promptly upon any instructions from a Data Subject to amend inaccurate or changed personal data.

1.6 Personal Data shall be kept in a form which permits identification of subjects for no longer than is necessary for the processing purpose. This means that staff will:

1.6.1 consider opportunities to de-personalise records, where appropriate, throughout their life cycle where deletion is not appropriate; and

1.6.2 follow the University Information Governance and Management Policy.

1.7 Personal Data shall be processed securely and in a manner that protects against unauthorised or unlawful processing, loss, destruction or damage. This means that staff will:

1.7.1 comply with the requirements of the University Information Governance and Management Policy and related regulations;

1.7.2 apply security controls to the processing of data, appropriate to the nature and sensitivity of that data, paying particular caution to the processing of special category or criminal conviction data;

1.7.3 take particular care when processing Personal Data at home or remotely as such processing presents an increased risk of loss, theft or damage to that data.

1.7.4 It is important that staff working on campus and those working remotely as in the case of work from home or working when travelling or any such remote work situation, should never share their access codes with anyone including work colleagues, family members and friends for the various technology applications that they use for work.

1.7.5 All staff must ensure that they log out of the various work-related technology applications when their device is unattended to avoid any uncalled-for data breaches.

1.7.6 Those using University devices must not share these devices with family or friends.

1.7.7 Those using their own devices for work must ensure that they ensure confidentiality of work-related data by securing passwords or access codes.

1.7.8 Use of removable media such as hard drives or flash drives is strictly prohibited, and any such use needs prior permission of the DPO and any such usage must be minimized and data should be erased at the earliest. The least secure method of manipulating corporate information remotely is to take a copy on a USB memory stick or other removable media. This should be used as a last resort as it is the most vulnerable to data loss and virus transmission.

1.8 The Data Controller shall be responsible for demonstrating compliance with the above principles. This means that staff will:

1.8.1 comply with all University policies, codes of practice and guidance relating to Information Governance;

1.8.2 if in doubt, seek advice from the Data Protection Officer before processing Personal Data;

1.8.3 promptly undertake all recommended and mandatory training programmes;

1.8.4 highlight concerns about any activity that may compromise the security and privacy of Personal Data;

1.8.5 Comply with any request by the Office of the Vice-Chancellor or the Data Protection Officer to assess compliance with and/or effectiveness of Information Governance and Management Policies, Codes of Practice and guidelines.

1.9 Prior to Personal Data being processed by another organisation on behalf of the University, the Office of the Vice-Chancellor must be consulted to ensure legislative compliance. In such cases, data protection impact assessments and contracts restricting use of Personal Data are likely to be required.

2 General requirements when processing Sensitive Data

2.1 Sensitive data is defined as encompassing any Personal Data consisting of an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life or sexual orientation.

2.2 Particular care must be taken with the processing of this category of Personal Data because of the greater potential impact to data subjects' privacy rights, and greater consideration given to how to process the Data securely.

2.3 Criminal Convictions data is to be treated as particularly sensitive data and handled in accordance with the legislation.

3 General requirements when processing Personal Data about children

3.1 It is important to afford additional protections to the Personal Data of individuals who are under-16.

4.1.1 Where processing of personal data of a child relates to the offer of information society services, such processing of personal data shall be lawful only to the extent that consent is given or authorised by a parent or person who has parental duties over the child in terms of the Children's Act.

4.1.2 For the purposes of 4.1.1 above, the data controller shall where appropriate and taking into account 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

3.2 Where the child is 16 years of age such child may give consent in such a manner as may be prescribed.

3.3 All involved staff must complete the following actions when implementing an activity involving the processing of child personal data:

3.3.1 Ensure any privacy information aimed at children is age appropriate and written in clear, plain language that a child or young person can understand;

3.3.2 Complete a Data Protection Impact Assessment Form to ensure that the appropriate technical and organisational measures have been implemented to protect this data;

4 General requirements for relying on Consent as a Lawful Basis

4.1 Where you are relying on Consent as your lawful basis for processing personal data you must ensure that the following applies:

4.1.1 A clear demonstration that the data subject has consented to the processing of his or her personal data.

4.1.2 If the data subject's consent is given in the form of a written declaration which also concerns other matters, the request for consent shall be presented —

- in a manner which is clearly distinguishable from the other matters; and
- in an intelligible and easily accessible form using clear and plain language.

4.1.3 The data subject is not under any undue pressure to consent to the processing activity and there is no clear imbalance of power between the University and the data subject;

4.1.4 The data subject is able to withdraw their consent at any time if they wish to do so, at which point, the University will cease the processing;

4.2 If any of the above actions cannot be achieved, an alternative lawful basis should be sought.

5 Privacy Notices

5.1 As set out above, in accordance with the principle of transparency, Data subjects must be informed of the nature and purpose of processing Personal Data that will take place.

5.2 This will normally be achieved in the form of a privacy notice. Privacy notices are required regardless of the nature or format of collection of Personal Data whether via paper forms, online forms, information provided verbally, or other means. The aim of the notice is to ensure that any subsequent processing can be "reasonably expected" by the individual.

5.3 As a minimum the following information must be provided in a privacy notice:

5.3.1 The identity of the Data Controller (the University, not an individual or a department);

5.3.2 the purpose for processing; the lawful ground for processing;

5.3.3 the length of time the Personal Data will be stored;

5.3.4 the use of any automated decision making (where relevant).

5.4 The University publishes core privacy notices on its website describing the processing which takes place in respect of students, staff and general users of the website. Specific privacy notices should be provided by all University services at the point of data collection, referring where appropriate to the General Privacy Notices.

5.5 If you are unsure whether a processing activity requires a privacy notice, or require assistance with wording a notice, please contact the Data Protection Officer.

5.6 Where a privacy notice is supplied to an individual, a record of that notice should be kept for as long as the Personal Data is retained, plus six years (should a legal claim be brought against the University). Where a privacy notice is altered, previous versions must also be maintained in line with the above.

5.7 If a privacy notice changes it may need to be re-communicated to data subjects.

5.8 In certain circumstances it may be necessary to provide a privacy notice and consent verbally. This must be documented, and where possible, legally recorded. To support users in complying with the data protection principles when collecting Personal Data, a useful checklist is provided at Annex A.

6 Data Protection Impact Assessments (DPIA)

6.1 It is important to minimise the unwarranted intrusions of privacy by designing systems which are robust and which ensure only data which is necessary for each specific purpose is processed and that technical and organisational measures are in place to ensure its security.

6.2 Where a project involves high risk processing a DPIA has to be carried out in accordance with the University's guidance on completing DPIAs. No processing may be carried out prior to this assessment being completed and the DPO authorising the processing.

6.3 You should conduct a DPIA in the following circumstances:

6.3.1 The use of new technologies;

6.3.2 Changing technologies (e.g.) programs, systems or processes;

6.3.3 Automated processing or profiling

6.3.4 Large scale systematic monitoring of a publicly accessible area

6.3.5 Large scale processing in particular of Sensitive personal data or personal data related to criminal convictions

6.3.6 When a processing operation requires a DPIA based on the list published by the Information and Data Protection Commission

6.4 A DPIA must include:

6.4.1 A description of the processing and its purpose;

6.4.2 The lawful basis for processing;

6.4.3 An assessment of the necessity and proportionality of processing in this way;

6.4.4 An assessment of the risks to individuals' privacy rights;

6.4.5 Risk mitigation in place to minimise any potential impact on privacy rights.

7 Storage and disposal of Personal Data

7.1 Personal Data must always be kept appropriately secured against damage or unauthorised access, amendment or deletion, with precautions taken appropriate to its confidentiality and sensitivity in line with the University's Information Governance and Management Policy.

7.2 Electronic and physical files containing Personal Data should have appropriate access restrictions in place so that only authorised individuals can gain access to them.

7.3 Personal Data must not be stored on portable media devices (e.g. memory sticks, DVDs) unless approval of the Data Protection Officer has been sought and appropriate safeguards put in place. There should be limited circumstances where this is required because of the nature of the University's network and provision of secure, remote working options.

7.4 Where the processing of Personal Data on a portable media device has been authorised by the Data Protection Officer, it must be encrypted using facilities provided by the University.

7.5 The use of hosted storage facilities (i.e. outside of the University's network) for Personal Data is not permitted unless:

7.5.1 The system is controlled by the University; or

7.5.2 Appropriate approval and advice has been sought from the Data Protection Officer, usually requiring a data protection impact assessment and contract.

7.6 Personal Data must not be kept for longer than is necessary. Be particularly aware of electronic databases building up indefinitely. The University's Record Retention Schedule guides the retention requirements for records relating to various activities.

7.7 Personal Data must be disposed of in a manner appropriate to its sensitivity. Records awaiting destruction must continue to be stored securely.

7.8 Paper waste that does not contain Personal Data may still be considered confidential, such as corporate or unit plans, financial information and anything that may have a negative commercial impact on the business if made available to unauthorised individuals.

7.9 Confidential paper data must also be disposed of in an appropriate manner including shredding.

7.10 Paper data that is not personal and not confidential should be placed in waste paper bins but if there is any uncertainty as to the confidentiality of paperwork it is best to err on the side of caution and use appropriate methods of disposal including shredding.

8 Disclosure and sharing of Personal Data with Third Parties

8.1 As a general rule, Personal Data may not be disclosed to any third party without the consent of the individual concerned or a defined and documented lawful basis for sharing. In this context "third parties" includes, but is not limited to, family members, friends, local authorities, government bodies and the police.

8.2 Requests for the disclosure of Personal Data from the Police, the Student Loans Agency, or from other official bodies and agencies must be referred to the Information Governance Team so that a lawful basis for sharing the information can be demonstrated. The exceptions to this are:

8.2.1 cases where the immediate disclosure of Personal Data is required by law enforcement or health care agencies for the imminent prevention of serious crime or the prevention of significant harm to an individual and advice from the Information Governance Team is unavailable (e.g. outside of standard working hours). Staff must take reasonable steps to verify the identity of the requestor, disclose only what is immediately necessary and document the details of the disclosure including the requestor contact details, purpose of request and information disclosed;

8.2.2 cases where faculties or departments have been authorised by the Information Governance Team to routinely handle disclosures directly, in which case specific procedures will be agreed.

8.3 Provision of references: When staff members are asked to provide references for students or other staff members, this request must be in writing and the reference document must follow the approved format where only the minimum required personal data is provided.

8.4 Personal Data can be shared within the University provided that such sharing is reasonable, necessary, not excessive, and is not incompatible with the original purpose for gathering the data.

8.5 When disclosing or discussing information about individuals, reasonable steps should be taken to verify the identity of the recipient, especially in telephone conversations or email correspondence. No information should be provided without a lawful basis for disclosing the information. Be aware of the risk of individuals posing as legitimate recipients in order to acquire information from the University.

8.6 When disclosing or sharing Personal Data, particular care must be given to the risks of correspondence being intercepted or errors in transmission. Only the minimum necessary information should be included and particular care must be taken when entering the recipient's details. If appropriate to the sensitivity of the information, email attachments can be password protected and/or encrypted.

9 Data Subjects

9.1 Data Subjects have a right to be informed of the Personal Data processed by the University about them. This is commonly known as a data subject access request or DSAR.

10.1.1 Such requests can be made free of charge, preferably in writing or by telephone to be followed up in writing and must be completed within one calendar month, or three calendar months in exceptional cases.

9.2 Data subjects wishing to exercise this right should be directed to place their request in writing to dpo@bothouniversity.ac.bw or by telephone.

9.3 Any request directed to an individual member of staff must be directed to the Information Governance Team without delay. The Information Governance Team will coordinate all requests for access to Personal Data, with the assistance of the faculty or department responsible for the information.

10 Personal Data Breaches

10.1 A Personal Data breach is considered to be any loss, damage or destruction to Personal Data or the unauthorised access, disclosure and/or processing of Personal Data.

10.2 Such incidents may cause unwarranted damage or distress to data subjects, generate negative media attention and/or constitute a breach of Data Protection Law for which the University can be subject to serious penalties.

10.3 Examples of Personal Data breaches include:

10.3.1 Loss or theft of devices or equipment on which Personal Data is stored e.g. a memory stick;

10.3.2 An email containing Personal Data sent to the wrong person;

10.3.3 Disclosure of Personal Data, via any method, to a third party such as a family member without consent or other legal power or obligation to do so;

10.3.4 Data Protection Law includes a requirement to report significant breaches within 72 hours.

10.3.5 To ensure that breaches can be investigated and managed with the legislative timeframes they must be reported by a Manager to the Information Governance Team without delay via dpo@bothouniversity.ac.bw or by telephone.

11 Transfers Outside the Republic of Botswana

11.1 Where it has been determined that Personal Data must be transferred outside of the Republic of Botswana this should be referred to the Information Governance Team in the first instance.

11.2 The Information Governance Team will advise whether any additional measures must be taken to ensure that the transfer of personal data is completed lawfully and involves minimal risk.

11.3 These additional measures may include the completion of:

11.3.1 A Data Protection Impact Assessment;

11.3.2 An International Data Transfer Agreement (IDTA)

11.3.3 A Transfer Risk Assessment (TRA)

12 Complaints

13.1 Any complaints, concerns or dissatisfaction regarding the University's processing of Personal Data must immediately be brought to the attention of the Data Protection Officer or the Office of Vice-Chancellor.

13 Contacts and Further Information

13.1 Queries relating to the processing of Personal Data or Data Protection Law should be referred to the Information Governance Team email: dpo@bothouniversity.ac.bw. The Information Governance Team referred to in this Code of Practice document is the Office of the Vice-Chancellor.

14 Annex A Personal Data Processing Checklist

This checklist should be used whenever there are plans to collect Personal Data for the first time or in respect of processing activities that are not already routinely carried out by the University.

Details	Yes/No	Notes
Is it necessary to collect this data?		
Have I checked if the processing of this data may have any negative impact on data subjects?		
Have I considered the possibilities of anonymising/pseudonymising this data?		
Is this processing covered by existing privacy notice to data subjects? Or should a new privacy notice be issued?		
Has the lawful bases of processing this data been identified as per the law?		
For sensitive personal data - has the lawful bases been identified as per the law?		
Is this processing recorded in the Record of Processing Activity for the University?		
What steps have I taken to ensure accuracy of data?		
Will this data be shared? With whom? Is there a Data Sharing Agreement in place? Has the data subject been informed?		
Will this data be transferred outside Botswana? Are all the necessary permissions in place?		
Is there a third-party data processor involved? Are all necessary contracts/notices in place?		
Are you aware of how long this data will be kept?		

If you have answered no to any of the above questions, contact the Information Governance Team before proceeding.