



General Data Protection Privacy Notice

Approving Authority	EMT
Date of Approval	25 th February 2026
Version #	1
Effective Date	26 th February 2026
Date last reviewed
Revision date(s)	
Responsible Officer	Manager - Data Protection
Document URL

1. INTRODUCTION

Botswana Open University (hereinafter "the University" or "BOU") is committed to protecting the privacy and personal data of all individuals who interact with the institution. This General Privacy Notice explains how we collect, use, share, store, and protect personal data in accordance with the Data Protection Act, 2024 (Act No. 9 of 2024) and other applicable laws in the Republic of Botswana.

1.1 Purpose of This Notice

This Notice is designed to provide transparency about our data processing activities and to inform you of your rights as a data subject under Botswana law. We are committed to processing personal data lawfully, fairly, and transparently, with appropriate safeguards to protect individual privacy and fundamental rights.

1.2 Scope and Application

This General Privacy Notice applies to all categories of individuals who interact with Botswana Open University, including:

- Students – prospective, current, and former students across all programmes and modes of study.
- Staff – employees, contractors, consultants, volunteers, and temporary workers
- Alumni – graduates and former students maintaining engagement with the University.
- Visitors – individuals visiting University premises, attending events, or accessing facilities.
- Research Participants – individuals participating in university-led research studies.
- Suppliers and Service Providers – contractors, vendors, and business partners.
- Job Applicants – individuals applying for employment or academic positions
- General Public – anyone interacting with the University through enquiries, website visits, or other channels.
- Specific privacy notices may supplement this General Notice for particular categories of data subjects (e.g., Student Privacy Notice, Staff Privacy Notice) or processing activities.

2. WHO WE ARE

2.1 Data Controller

Botswana Open University is the data controller responsible for determining the purposes and means of processing personal data.

Garamothlose Junction,
Western Bye-Pass, Block 6,
Plot 39972
Gaborone,
Botswana

Website: www.bou.ac.bw
Tel: (+267) 3646000
Email: enquiries@staff.bou.ac.bw

2.2 Data Protection Manager

The University has appointed a Data Protection Manager responsible for overseeing compliance with the Data Protection Act, 2024, and serving as the primary point of contact for data protection matters.

Email: dpo@bou.ac.bw
Telephone: +267 3646053
Office Hours: Monday–Friday, 07:30–16:30

You may contact the Data Protection Officer for:

- Questions about how your personal data is processed
- Requests to exercise your data subject rights
- Concerns about data protection compliance
- Reporting suspected data breaches or privacy incidents

3. WHAT PERSONAL DATA WE COLLECT

The University collects various categories of personal data depending on the nature of your relationship with the institution. The following provides an overview of the main categories:

3.1 Basic Identification and Contact Information

- Full name, title, and preferred name
- National identification number (Omang), passport number, or other government-issued ID
- Date of birth, age, and nationality
- Gender and marital status
- Contact details (residential and postal addresses, telephone numbers, email addresses)
- Photographs and video recordings
- Emergency contact information (names, relationships, contact details of next of kin)

3.2 Academic and Educational Data

- Educational qualifications, transcripts, and certificates
- Previous institutions attended and academic references
- Programme of study, course selections, and registration records
- Assessment submissions, examination scripts, and academic results
- Grades, classifications, and awards conferred
- Attendance records and academic engagement data
- Learning Management System (LMS) activity and analytics
- Academic misconduct records and disciplinary matters
- Thesis, dissertation, and research outputs
- Student feedback, evaluations, and surveys

3.3 Employment and Human Resources Data

- Employment application materials (CV, cover letters, references)
- Employment contracts, job descriptions, and terms of service
- Position, title, department, and reporting structure
- Work history, qualifications, and professional registrations
- Salary, benefits, allowances, and pension information
- Performance appraisals, development plans, and training records
- Absence records (sick leave, annual leave, special leave)
- Disciplinary records and grievance documentation
- Termination records and exit interviews
- Trade union membership (where disclosed)

3.4 Financial and Payment Data

- Bank account details and payment information
- Tuition fee records, payment history, and outstanding balances
- Scholarship, bursary, loan, and sponsorship information
- Salary, allowances, deductions, and tax information
- Procurement records and vendor payment details
- Expense claims and reimbursement requests
- Donation records (for alumni and supporters)

3.5 Technical and IT Systems Data

- IP addresses, device identifiers, and browser information
- System login credentials and authentication records
- Network usage logs and access patterns
- Email communications sent through University systems
- Virtual Learning Environment (VLE) access and usage data
- Library system borrowing records and resource access
- CCTV footage and access control records
- Cybersecurity monitoring and incident logs

3.6 Special Category Personal Data

In accordance with Section 25 of the Data Protection Act, 2024, the University processes special categories of personal data (sensitive data) only where there is a lawful basis and appropriate safeguards are in place. Special category data includes:

- Health and medical information – medical conditions, disabilities, mental health status, medication requirements, occupational health assessments
- Disability and accessibility needs – physical, sensory, learning, or cognitive disabilities requiring reasonable accommodations
- Racial or ethnic origin – collected for equal opportunities monitoring, diversity reporting, and affirmative action compliance
- Religious or philosophical beliefs – for accommodation of dietary requirements, prayer facilities, or religious observances
- Biometric data – fingerprints or facial recognition data for secure access control and identity verification
- Trade union membership – where disclosed for payroll deductions or employee representation
- Criminal conviction and offence data – for vetting purposes related to work with vulnerable populations, professional registration requirements, or campus security.

Processing of special category data is conducted with explicit consent where required, or where otherwise lawful under the Data Protection Act (e.g., vital interests, public interest, legal claims, substantial public interest).

3.7 Research Data

- Participation consent forms and information sheets
- Research questionnaires, interviews, and survey responses
- Observational data and field notes
- Biological samples or genetic information (where applicable)
- Any other data collected as part of University-led research studies

3.8 Visitor and Event Attendance Data

- Names and contact details of campus visitors
- Purpose of visit and host information
- Vehicle registration numbers (for parking and security)
- Event registration and attendance records
- Dietary preferences and accessibility requirements for events

4. WHY WE USE YOUR PERSONAL DATA

Botswana Open University processes personal data to support the delivery of its core functions as a public institution of higher education and research. The specific purposes for which we process personal data include:

4.1 Academic Administration and Student Services

- Processing applications for admission, enrolment, and registration
- Administering academic programmes, courses, and learning activities
- Conducting assessments, examinations, and awarding qualifications
- Monitoring academic progress, engagement, and attendance
- Providing academic support, tutoring, and counselling services
- Managing student accommodations, disability support, and welfare services
- Facilitating graduation ceremonies and issuing certificates and transcripts
- Administering alumni relations and lifelong learning opportunities
- Verifying academic credentials and providing references

4.2 Human Resources and Employment Management

- Recruiting, selecting, and appointing staff members
- Administering employment contracts and terms of service
- Processing payroll, benefits, pensions, and tax obligations
- Managing performance appraisals, promotions, and career development
- Providing occupational health services and managing workplace safety
- Processing leave applications, absence records, and flexible working arrangements
- Investigating and resolving disciplinary matters, grievances, and complaints

- Managing terminations, retirements, and post-employment obligations
- Maintaining staff records for pension and reference purposes

4.3 Financial Administration and Resource Management

- Processing tuition fees, scholarships, bursaries, and loans
- Managing vendor payments, procurement, and contracts
- Processing expense claims and reimbursements
- Conducting financial audits and budget management
- Administering donations, fundraising, and development activities
- Managing University assets, facilities, and resources
- Ensuring compliance with financial regulations and tax laws

4.4 Compliance and Legal Obligations

- Meeting requirements under the Data Protection Act, 2024

- Complying with labor laws, employment regulations, and tax legislation
- Fulfilling obligations to regulatory and accreditation bodies
- Responding to court orders, subpoenas, and legal requests
- Cooperating with law enforcement and government agencies
- Managing legal claims, disputes, and litigation
- Maintaining records for audit, inspection, and accountability purposes

4.5 Communication and Stakeholder Engagement

- Communicating with students, staff, and stakeholders about University matters
- Sending newsletters, announcements, and event invitations
- Conducting surveys and seeking feedback to improve services
- Managing media relations and public communications
- Marketing and promoting University programmes, research, and achievements
- Engaging with alumni and maintaining lifelong relationships
- Facilitating community outreach and public engagement activities

4.6 Security, Safety, and Risk Management

- Ensuring campus security and access control
- Monitoring premises through CCTV and surveillance systems
- Preventing and detecting fraud, unauthorized access, and misconduct
- Protecting IT systems from cyber threats and security incidents
- Managing health and safety risks and emergency situations
- Conducting security vetting where required for sensitive positions or research
- Investigating incidents, accidents, and security breaches

4.7 Research and Institutional Planning

- Conducting academic, scientific, and policy research
- Analyzing institutional data for quality assurance and improvement
- Supporting strategic planning, forecasting, and decision-making
- Producing statistical reports for internal and external stakeholders
- Benchmarking performance against national and international standards
- Archiving records for historical and public interest purposes

All processing activities are carried out lawfully, fairly, and transparently, with appropriate safeguards to protect the privacy, dignity, and rights of individuals.

5. LEGAL BASIS FOR PROCESSING

Under the Data Protection Act, 2024, personal data may only be processed where there is a lawful basis. The University relies on the following legal bases depending on the nature and purpose of processing:

5.1 Contractual Necessity

Processing is necessary for the performance of a contract to which the data subject is a party, or to take steps at the request of the data subject prior to entering into a contract.

Examples:

- Processing student enrolment and registration
- Administering employment contracts and payroll
- Delivering teaching, learning, and assessment services
- Providing accommodation and facilities

5.2 Legal Obligation

Processing is necessary for compliance with a legal obligation to which the University is subject under Botswana law or other applicable legislation.

Examples:

- Complying with tax and financial reporting requirements
- Meeting statutory obligations under employment and labor laws
- Responding to court orders, subpoenas, and regulatory requests
- Reporting to government agencies (e.g., immigration, education ministry)
- Implementing health and safety regulations

5.3 Performance of a Task in the Public Interest

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 University.

Examples:

- Providing public education and research
- Awarding qualifications and certifications
- Contributing to national development and skills training
- Conducting research for public benefit
- Maintaining academic standards and quality assurance

5.3 Legitimate Interests

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

Examples:

- Fraud prevention and detection
- Network and information security
- Alumni engagement and fundraising activities
- Institutional research and planning

- CCTV surveillance for campus security

- Direct marketing (subject to opt-out rights)

Before relying on legitimate interests, the University conducts a balancing test to ensure that the processing is proportionate and does not unduly infringe on individual rights.

5.4 Vital Interests

Processing is necessary to protect the vital interests (life or physical integrity) of the data subject or another natural person.

Examples:

- Medical emergencies requiring immediate intervention
- Safeguarding vulnerable individuals from harm
- Responding to threats to life or safety

5.6 Consent

The data subject has given explicit, informed, and freely given consent to the processing of their personal data for one or more specific purposes.

Examples:

- Processing special category data (health, ethnicity, religious beliefs)
- Using photographs or video recordings for marketing purposes
- Sending promotional communications (where not based on legitimate interests)
- Participation in optional research studies

Where consent is relied upon, individuals have the right to withdraw consent at any time without affecting the lawfulness of prior processing.

6. WHO WE SHARE YOUR DATA WITH

The University may share personal data with third parties where it is lawful, necessary, and proportionate to do so. Data sharing is conducted in accordance with the Data Protection Act, 2024, and subject to appropriate safeguards.

6.1 Government Bodies and Regulatory Authorities

- Ministry of Education and Skills Development – for national education statistics, policy development, and regulatory compliance
- Department of Tertiary Education Funding (DTEF) – for funding administration, attendance verification, and progress reporting
- Botswana Qualifications Authority (BQA) – for programme accreditation, quality assurance, and qualifications verification
- Botswana Unified Revenue Service (BURS) – for tax compliance and reporting
- Immigration authorities – for visa sponsorship and compliance with immigration laws
- Statistics Botswana – for national statistics (anonymized or aggregated where

possible)

- Botswana Police Service and DCEC – where required for law enforcement, crime prevention, or investigation
- Information and Data Protection Commission – for regulatory compliance and investigation of complaints

6.2 Educational Partners and Accreditation Bodies

- Partner universities and institutions – for student exchanges, joint programmes, credit transfers, and research collaborations
- Examination boards and awarding bodies – for qualification verification and external examining
- Professional registration bodies – for licensing, accreditation, and professional standards compliance
- Quality assurance agencies – for institutional audits and programme reviews

6.3 Service Providers and Data Processors

The University engages third-party service providers to perform functions on its behalf. These processors are contractually bound to:

- Process data only on documented instructions from the University
- Implement appropriate security measures
- Maintain confidentiality
- Assist with data subject rights requests
- Delete or return data upon contract termination

Examples of service providers:

- Cloud hosting and IT infrastructure providers
- Student information system providers
- Email and communication platform providers
- Plagiarism detection services (e.g., Turnitin®)
- Payment processors and banking services
- Security and facilities management contractors
- Occupational health and medical service providers
- Legal advisors, auditors, and consultants

6.4 Law Enforcement, Legal, and Security Entities

- Courts and tribunals – in response to court orders, subpoenas, or legal proceedings
- Law enforcement agencies – for crime prevention, detection, investigation, or prosecution
- Legal advisors and solicitors – for legal advice, representation, and litigation
- Insurance companies – for managing claims and policy administration
- Debt collection agencies – for recovery of outstanding fees or debts

6.5 Sponsors, Employers, and Placement Providers

- Scholarship providers and sponsors – to confirm enrolment, attendance, and academic progress
- Employers – for work-integrated learning, internships, and employment verification
- Placement providers (hospitals, schools, industry partners) – for practical training and supervision

6.6 Parents, Guardians, and Next of Kin

Disclosure to parents, guardians, or next of kin occurs only:

- With explicit consent of the data subject
- In emergencies involving vital interests
- Where the data subject is a minor (under 18 years)

As required by law

6.7 Other Third Parties

- Research collaborators and funding agencies – for collaborative research projects
- Alumni networks and professional associations – for networking and engagement
- Event organizers and venue providers – for conferences, ceremonies, and events

6.8 Safeguards for Data Sharing

All data sharing is subject to:

- Contractual agreements incorporating data protection clauses
- Confidentiality obligations and non-disclosure agreements
- Security requirements and technical safeguards
- Purpose limitation – data shared only for specified purposes
- Data minimization – sharing only necessary information
- Accountability measures – monitoring and auditing compliance

7. INTERNATIONAL TRANSFERS OF PERSONAL DATA

7.1 When International Transfers Occur

Botswana Open University may transfer personal data outside the Republic of Botswana in the following circumstances:

- Cloud services and IT infrastructure hosted on international servers

- International partnerships and collaborations with universities and research institutions
- Student exchanges and study abroad programmes
- International research collaborations and data sharing
- Service providers operating across borders (e.g., Turnitin®, LMS platforms, email services)
- International conferences, publications, and academic activities

7.2 Safeguards for International Transfers

Where personal data is transferred to countries that do not have data protection laws equivalent to those in Botswana, the University ensures that appropriate safeguards are in place, including:

- Standard contractual clauses approved by the Information and Data Protection Commission or recognized international frameworks
- Adequacy decisions where the destination country is deemed to provide adequate protection
- Binding corporate rules for transfers within multinational organizations
- Certification mechanisms and codes of conduct
- Explicit consent from data subjects where other safeguards are not available

The University conducts transfer impact assessments to evaluate risks and ensure adequate protection for international data transfers.

8. HOW LONG WE KEEP YOUR DATA

8.1 Retention Principles

Personal data is retained only for as long as necessary to fulfil the purposes for which it was collected, including compliance with legal, regulatory, audit, and accountability requirements. The University's retention practices are guided by:

- The Data Protection Act, 2024
- The University's approved Records Retention and Disposal Schedule
- Legal and regulatory requirements
- Legitimate business needs and institutional purposes

Detailed retention periods are specified in the University's Records Retention and Disposal Schedule, available from the Data Protection Officer.

8.3 Secure Disposal

At the end of the retention period, personal data is securely disposed of through:

- Electronic data: Secure deletion, data wiping, or destruction of storage media
- Paper records: Confidential shredding or incineration

- Portable devices: Physical destruction or degaussing

8.4 Anonymization and Archiving

In certain circumstances, personal data may be anonymized so that it can no longer be linked to an identifiable individual. Anonymized data may be retained indefinitely for research, statistical analysis, or archiving in the public interest.

9. YOUR RIGHTS UNDER THE DATA PROTECTION ACT

As a data subject, you have the following rights under the Data Protection Act, 2024:

Right	What This Means	How to Exercise
Right of Access	You can request confirmation of whether we process your personal data and obtain a copy of that data.	Submit a Data Subject Access Request (DSAR) to the DPO with proof of identity.
Right to Rectification	You can request correction of inaccurate, misleading, or incomplete personal data.	Submit a rectification request to the DPO with supporting documentation.
Right to Erasure ("Right to be Forgotten")	You can request deletion of personal data in certain circumstances (e.g., data no longer necessary, consent withdrawn, unlawful processing).	Submit a written erasure request to the DPO specifying the data and grounds.
Right to Restriction of Processing	You can request that we limit processing while accuracy is verified, legality is assessed, or legal claims are considered.	Submit a restriction request to the DPO outlining the basis.
Right to Data Portability	You can receive your personal data in a structured, machine-readable format and transmit it to another controller.	Submit a portability request to the DPO (applies only to automated processing based on consent or contract).
Right to Object	You can object to processing based on legitimate interests or for direct marketing purposes.	Submit a written objection to the DPO stating your grounds.
Right to Withdraw Consent	Where processing is based on consent, you can withdraw it at any time without affecting prior lawful processing.	Submit a withdrawal notice to the DPO or through the platform where consent was provided.
Right Not to Be Subject to Automated Decision-Making	You can request human review of decisions made solely by automated means that produce legal or significant effects.	Submit a request to the DPO for human intervention and explanation.
Right to Lodge a Complaint	You can complain to the Information and Data Protection Commission if you believe your rights have been violated.	Contact the Commission and notify the DPO.

9.1 Response Time

The University will respond to data subject rights requests within 30 days of receipt. This period may be extended by an additional 60 days where requests are complex or numerous, with notification and justification provided to the data subject.

9.2 Limitations on Rights

Certain rights may be subject to limitations or exemptions where:

- Processing is necessary for legal obligations or public interest tasks
- Disclosure would adversely affect others' rights
- Information is subject to legal privilege

- Processing is necessary for legal claims or regulatory compliance

The University will explain any limitations when responding to your request.

9.3 How to Exercise Your Rights

To exercise any of your rights, please contact:

Data Protection Manager
Botswana Open University
Email: dpo@bou.ac.bw
Telephone: +267 3646053

Please provide:

- Clear identification of the right you wish to exercise
- Proof of identity (Oman, passport, or student/staff ID)
- Specific details about your request
- Preferred method of response

There is no fee for exercising your rights unless requests are manifestly unfounded, excessive, or repetitive, in which case a reasonable administrative charge may apply.

10. DATA SECURITY

10.1 Our Commitment to Security

Botswana Open University takes the security of personal data seriously and implements appropriate technical and organizational measures to protect against unauthorized access, accidental loss, destruction, alteration, or disclosure.

10.2 Technical Security Measures

- Encryption – Data transmission via SSL/TLS; encryption of sensitive data at rest
- Firewalls and network security – Multi-layered protection against cyber threats
- Access controls – Role-based access ensuring only authorized personnel can access data
- Authentication – Strong password policies, multi-factor authentication (MFA)
- Secure storage – Protected servers, encrypted cloud storage, access logging
- Data backup and disaster recovery – Regular backups with tested recovery procedures
- Antivirus and anti-malware – Real-time threat detection and prevention
- Security monitoring – Continuous monitoring for suspicious activity and breaches
- Vulnerability assessments – Regular testing and remediation of security weaknesses

10.3 Organizational Security Measures

- Data protection policies and procedures governing data handling
- Staff training and awareness on data protection responsibilities
- Confidentiality agreements for all staff and contractors
- Data Protection Impact Assessments (DPIAs) for high-risk processing
- Incident response plan for detecting and responding to breaches
- Regular security audits – Internal and external assessments
- Physical security – Secure facilities, restricted access, CCTV surveillance

10.4 Data Breach Notification

In the event of a personal data breach likely to result in a risk to the rights and freedoms of data subjects, the University will:

- Notify the Information and Data Protection Commission without undue delay and, where feasible, within 72 hours
- Notify affected data subjects where the breach poses a high risk
- Document the breach, including facts, effects, and remedial actions
- Investigate and implement measures to prevent recurrence

To report a suspected data breach, contact the Data Protection Officer immediately at dpo@bou.ac.bw or +267 3646053.

11. UPDATES TO THIS PRIVACY NOTICE

This General Privacy Notice may be updated periodically to reflect:

- Changes in data protection laws or regulations
- New processing activities or technologies
- Organizational restructuring or operational changes
- Best practices and guidance from regulatory authorities
- The current version of this Notice is effective from 01 January 2026 and will be reviewed at least annually.

Notice of Changes:

- Material updates will be published on the University website (www.bou.ac.bw)
- Current students and staff will be notified via email
- The "Date Last Reviewed" field will reflect the most recent update

Continued interaction with the University following notification of changes constitutes acceptance of the revised Notice.

12. CONTACT INFORMATION

For General Enquiries

Email: enquiries@staff.bou.ac.bw

Telephone: (+267) 3646000

Website: www.bou.ac.bw

For Data Protection Matters

Data Protection Manager
Garamotlhose Junction,
Western Bye-Pass, Block 6,
Plot 39972
Gaborone,
Botswana

Email: dpo@bou.ac.bw

Telephone: +267 3646053 or +267 72280485

Office Hours: Monday–Friday, 07:30–16:30

To Lodge a Complaint

If you believe your data protection rights have been violated, you may lodge a complaint with:

Information and Data Protection Commission

You are encouraged to contact the University's Data Protection Office first to allow us to address your concerns directly.

END OF DOCUMENT

This General Privacy Notice has been prepared in compliance with the Data Protection Act, 2024 (Act No. 9 of 2024) and reflects Botswana Open University's commitment to protecting the privacy and personal data of all individuals.