Policy Title	Student Data Protection Policy
Version	№ 1
Effective Date:	September 15th , 2025
Approved by:	Academic Council
Scope:	University wide
Purpose:	To set out the ground rules for handling and using student data across all BMU departments

Student Data Protection Policy and Procedure

1. Purpose and Scope

Purpose: This policy outlines how British Management University (BMU) protects student personal data and ensures compliance with data protection laws. BMU is committed to safeguarding personal information and upholding the privacy rights of individuals in line with all applicable laws, including Uzbekistan's Law on Personal Data (2019).

Scope: This policy and procedure apply to all BMU students, employees, faculty, contractors, and any other parties who handle student personal data. It covers all forms of student data processing (electronic, paper-based, and other formats) conducted by or on behalf of BMU.

2. Key Definitions

Personal Data: Any information relating to an identified or identifiable individual (the "data subject"). This includes, for example, contact details, identification numbers, student records, and any information that can be linked to a student. (Note: Truly anonymized data, where individuals cannot be identified, is not considered personal data.)

Processing: Any action performed on personal data, whether automated or manual. Processing includes collecting, recording, organizing, storing, altering, retrieving, using, disclosing, transmitting, deleting, or destroying personal data.

Data Subject: An individual whose personal data is processed. In this context, typically a student (or prospective student) of BMU.

Data Controller: An organization or person that determines the purposes and means of processing personal data. BMU acts as the data controller for student data it holds.

Data Processor: An organization or person (other than a BMU employee) that processes personal data on behalf of the controller. For example, a third-party service handling student data under BMU's instructions would be a processor.

3. Roles and Responsibilities

All Staff and Faculty: Every BMU employee and faculty member is responsible for protecting personal data they handle. Staff must follow this policy and related procedures, attend required data protection training, and report any data breaches or incidents to the Academic Registrar and/or Dean immediately. All staff are expected to ensure that any personal data they work with is kept secure and confidential.

Students: Students must also adhere to this policy when they handle personal data (for instance, a research project involving personal information). Students should seek guidance if they are unsure how to protect personal data and must report any data-related incidents or concerns to faculty.

Third-Party Contractors and Partners: Any third parties who process student data on BMU's behalf must agree to comply with data protection requirements. BMU will ensure that proper agreements are in place with these parties, outlining their responsibilities to protect personal

data and maintain confidentiality. No contractor or partner should access or use student data beyond the purposes authorized by BMU.

4. Compliance with Policy

This policy is mandatory for all BMU employees, faculty, students, contractors, and any others authorized to access student data. Compliance with data protection principles is a condition of employment for staff and a condition of enrollment for students.

Employee Obligations: All employees and contractors must abide by this policy and related procedures as part of their employment or service conditions. Failure to do so may result in disciplinary action.

Student Obligations: By enrolling at BMU, students agree to follow University policies, including data protection rules, especially when their coursework or activities involve handling personal data.

Consequences of Breach: Any violation of this policy may result in corrective measures such as retraining, unless the breach is serious, in which case disciplinary measures may apply. For staff, this could include actions up to termination of employment. For students, it could include academic or disciplinary sanctions under the student code of conduct. BMU may also suspend or terminate contracts with third parties who fail to comply.

Legal Compliance: BMU will cooperate with regulatory authorities as required. Non-compliance with data protection law can lead to legal penalties for the University and individuals. Therefore, everyone covered by this policy must understand and fulfill their responsibilities to protect data.

5. Data Protection Principles

BMU adheres to the core principles of data protection as outlined below:

Lawfulness, Fairness, and Transparency: We only collect and process personal data if we have a valid legal basis and a legitimate purpose for doing so. Personal data must be processed fairly and not used in ways that are unreasonably intrusive or misleading.

Purpose Limitation: Personal data is collected for specific, explicit, and legitimate purposes. We will not use student data for purposes that are incompatible with the original reason it was collected. If we need to use data for a new purpose, we will either obtain the student's consent or ensure we have another lawful basis for the new use, and we will inform the student if required.

Data Minimization: We only collect the personal data that is adequate, relevant, and limited to what is necessary for the purpose. In other words, BMU will not ask for or keep more information about students than we truly need. Unnecessary data (especially sensitive information) is avoided.

Accuracy: BMU will keep personal data accurate and up to date. We encourage students to inform us of any changes to their personal information. Inaccurate or outdated data will be corrected or erased without delay.

Storage Limitation: We retain personal data only for as long as it is needed to fulfill the purposes for which it was collected (and to meet any legal or operational requirements). When data is no longer required, we will dispose of it securely, through deletion or shredding of records, to prevent unauthorized access.

Integrity and Confidentiality (Security): We protect personal data against unauthorized or unlawful access, loss, or disclosure. Appropriate technical and organizational security measures are in place to safeguard student data. This includes measures such as password protection on systems, encryption of sensitive data, access controls to limit who can view information, and

secure storage for physical records. Confidentiality is paramount: anyone handling student data must keep it confidential and not disclose it to anyone who is not authorized.

Accountability: BMU takes responsibility for complying with these principles and can demonstrate compliance. The University's leadership oversee adherence to this policy. We will also provide training and guidance to staff to ensure they understand their duties under this policy.

(All staff and students should familiarize themselves with these principles. If you have questions about how to apply them, contact the Academic Registrar and/or Deans for guidance.)

6. Obtaining and Using Student Data

When collecting or using student personal data, BMU staff and faculty should follow these guidelines:

Collection of Data: Wherever possible, collect personal data directly from the student. Ensure the student knows why their data is being collected. For example, when students fill out enrollment forms or provide information to Student Services, we will explain how their data will be used (through a privacy notice or form description).

Use and Disclosure: Use student data only for legitimate University purposes. Do not access or use a student's personal information out of curiosity or for non-work-related reasons. Personal data should only be shared with those within BMU who need it to perform their duties. If data needs to be shared with an external party (for instance, a partner university or a service provider), refer the section on data sharing. In all cases, ensure any use of data aligns with the original purpose of collection (or a compatible purpose as allowed by law).

Special Category Data: Extra caution is required when handling sensitive personal data (e.g., health records or data about a student's ethnicity or religion). Such data should only be collected if absolutely necessary and must be protected with higher security (for example, stored in encrypted files or locked cabinets, with access limited to specifically authorized personnel). In many cases, processing special category data requires the student's explicit consent or must meet other specific legal criteria.

7. Data Security and Access Control

BMU takes data security very seriously. We implement physical, technical, and administrative measures to ensure the safety and confidentiality of student personal data throughout its lifecycle (from collection to destruction):

Access Control: Access to student personal data is restricted to authorized personnel who need the information to perform their duties. Every staff member should only access and use the minimum data necessary for their task ("need-to-know" basis). User accounts, passwords, and permission levels are managed to prevent unauthorized access. No staff member should view or handle student data unless it is required for their job. If you are unsure whether you should have access to certain information, consult Academic Registrar and/or Dean.

Secure Storage: Personal data in electronic form is stored on secure BMU systems. This includes using password-protected databases, encrypted storage for sensitive information, and regular backups of critical data. Personal data should never be stored on unauthorized personal devices or emailed to personal accounts. Cloud services or external storage must be university-approved and compliant with data protection standards. Physical documents containing personal data (such as printed forms or reports) must be kept in locked cabinets or secure areas when not in use.

Data Transmission: When transmitting personal data (e.g., sending student information via email or sharing files), staff must use secure methods. Avoid using public or unsecured networks for transmitting confidential data.

Preventing Data Loss: BMU uses security software and protocols to prevent, detect, and respond to threats (such as firewalls, anti-virus programs, intrusion detection, etc.). Staff should be vigilant and follow IT guidelines: for example, do not plug in unknown USB drives, do not install unauthorized software, and report any suspicious computer activity. Regular audits and monitoring may be conducted to ensure security measures are effective.

Data Breach Response: In the event of a data breach (such as a lost laptop containing student data, a cyber-attack, accidental disclosure of student information, etc.), it must be reported immediately to the Academic Registrar and/or Dean and the IT department. A data breach is any incident that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. All staff have a duty to report breaches or suspected breaches without delay to their line manager. The sooner BMU is aware, the faster we can act to mitigate harm. The Registrar and Deans, together with relevant departments, will investigate the breach and take appropriate action. This includes containing the breach, recovering data if possible, and assessing risks to affected individuals. We will also document all breaches, even those not legally required to be reported, as part of our accountability. All breaches must be reported immediately, and no later than 24 hours, to the Academic Registrar and/or Dean. External reporting to regulators will be carried out where legally required.

Ongoing Evaluation: BMU continually evaluates and updates its security practices. We stay informed about new security threats and best practices, and we adapt our measures accordingly. Regular mandatory training should be provided to employees to keep everyone aware of how to handle personal data safely (e.g., training on recognizing phishing emails, using strong passwords, etc.). The University may also conduct periodic assessments or audits of data protection measures to ensure continued compliance and effectiveness.

8. Data Sharing and Disclosure

Sharing student data with third parties must be done cautiously and only in line with this policy and legal requirements:

Internal Sharing: Within BMU, student personal data should only be shared among staff/faculty who have a legitimate need for it. For example, an academic department may share student contact details with the student services office for official purposes, but broad or unnecessary sharing of data is prohibited. Always consider confidentiality – even within the University, avoid casually discussing or revealing personal information to those who have no role in that matter.

External Sharing: We do not disclose student personal data to external individuals or organizations unless we have a valid reason and, where required, the student's consent or another lawful basis. Common reasons for sharing externally might include: verification requests from other educational institutions or employers (with student consent), legal requirements (such as providing data to government education authorities or regulators), or service providers who assist BMU (such as an external learning platform or cloud service hosting student data). In all cases, BMU will ensure that any external party receiving student data is obligated to protect that data.

Data Transfer Abroad: If student personal data needs to be transferred outside of Uzbekistan (for example, to an international partner or a cloud server in another country), BMU will follow applicable data transfer regulations. We will ensure that the destination country has an adequate level of data protection or implement appropriate safeguards (such as standard contractual clauses or other approved mechanisms).

Legal Disclosures: If BMU is required by law to disclose student data (for instance, by a court order or law enforcement request), we will verify the request's authenticity and scope. Only the minimum necessary data will be disclosed, and the student will be informed of the disclosure unless we are legally forbidden from doing so.

No Unauthorized Sharing: Apart from the scenarios above, BMU will not sell, rent, or otherwise release student personal information to third parties. In particular, we do not provide student data to external companies for marketing or other purposes without explicit consent from the student. Any staff member found to be sharing student data inappropriately or without authorization will face disciplinary action.

9. Policy Awareness and Training

BMU will ensure that all relevant persons are aware of this Student Data Protection Policy:

Training: The University shall provide regular training sessions and materials on data protection and privacy best practices. All staff must complete mandatory data protection training (for example, an annual refresher course) to stay up to date on laws, this policy, and practical steps for compliance. New employees will receive training as part of their induction. The Registrar's Office is responsible for tracking compliance with annual training, with Deans and Vice-Rectors involved in the designed delivery of such training sessions.

Policy Access: This policy document is available on the BMU SRS. Students and staff will be notified of any significant updates to the policy.

Acknowledgement: Staff may be required to sign an acknowledgment that they have read and understood this policy (including the Communication Standards). Students may similarly be informed via student handbooks or orientation that this policy governs the handling of their personal data.

Students will be required to provide explicit acknowledgement of this policy during enrolment and orientation, confirming their understanding and acceptance.

10. Policy Enforcement and Disciplinary Action

Adherence to this policy is crucial for legal compliance and for maintaining trust with our students and community. BMU will enforce this policy through the following means:

Monitoring: BMU may monitor compliance with data protection procedures (for instance, audits of data access logs, checks on data sharing practices, or reviewing how confidential communications are handled). This is done in accordance with employment policies and applicable laws.

Incident Handling: If a potential breach of this policy is reported or detected (whether it's an unauthorized data disclosure, mishandling of sensitive information, or improper communication as per this policy), BMU will investigate the matter. The investigation may involve the Academic Registrar, Deans, IT Services, HR, and management as appropriate.

Consequences: If an investigation confirms that a staff member, student, or contractor violated the Student Data Protection Policy, BMU will take appropriate action. Consequences may include retraining, a formal warning, suspension, or up to termination of employment/contract for serious or deliberate violations. In the case of students, misconduct in handling personal data could result in disciplinary action under the student conduct code. BMU will also consider whether any breach needs to be reported to external authorities or regulators.

Legal Implications: Individuals should be aware that mishandling personal data can not only lead to internal discipline but also legal consequences. Under data protection laws, certain wrongful disclosures or misuse of personal data could result in fines or personal liability. BMU will not hesitate to report unlawful activities to the authorities if required.

11. Review and Maintenance of Policy

This policy (including the procedures and standards outlined) will be reviewed on a regular basis to ensure it remains up-to-date with current laws and best practices. At a minimum, an annual review will be conducted, and the policy will be updated as needed. Any changes will

be approved by BMU's senior leadership or Policy Committee. Major updates or additions will be communicated to all staff and students.

BMU is committed to continuous improvement in data protection. We welcome feedback on this policy. If you have suggestions to enhance data privacy or security at BMU, please contact the Academic Registrar and/or Deans. Regular reviews and community feedback help us maintain an effective policy that serves its purpose and is easy to follow.

Revision History

Version	Approved by	Approval Date	Description of Change
1	Academic Council	October 17, 2025	

Rector: Yuri Loktionov