Policy Title	BMU Communication Policy
Version	№ 1
Effective Date:	September 15th , 2025
Approved by:	Academic Council
Scope:	University wide
Purpose:	To set out the ground rules for both internal and external communication practices at BMU

Communication Policy

Purpose and Scope

This policy applies to all staff, teachers, students, interns, contractors, and any other employees handling University information.

This policy sets the standards for all forms of communication at BMU – including email, written documents, and verbal exchanges – to ensure professionalism, clarity, and confidentiality. It complements the University's Student Data Protection Policy by applying those same principles to everyday communication.

Key Principles

Confidentiality: Protect sensitive information at all times. Internal communications and documents are confidential and must not be disclosed to unauthorized individuals.

Integrity: Ensure information is accurate and only shared through secure and approved channels. Do not alter or misrepresent data in communication.

Accountability: Every staff member is responsible for safeguarding information. Report any data breaches or misdirected communications immediately to the appropriate authority.

Communication Guidelines

Email Communication

Email and Student Records System are the primary communication channels. All official communications should be conducted via company-provided email accounts. When using email, staff must adhere to the following best practices:

- Use official email only: Always use your official work email for work-related communications. Do not use personal email accounts (e.g., Gmail) to send or receive work documents or sensitive information.
- Confidentiality in emails: Treat all internal emails as confidential. Do not forward or share internal emails or their attachments with external parties (or anyone not authorized to view the information) without explicit permission. In particular, internal staff correspondence should never be shared with students or external individuals unless it's part of an approved process. Exceptions: forwarding may be permitted only when required by an authorized committee, regulator, or other formally approved body.
- Proper recipient handling: Double-check recipient addresses before sending an email, especially when the content is sensitive. Use "Bcc" (blind carbon copy) for group emails to external recipients (e.g. multiple students) to protect their email privacy and prevent accidental "Reply All" disclosures.

- Minimal data sharing: Share personal or sensitive data via email only on a need-to-know basis. Avoid including unnecessary personal details in emails. If you must send sensitive data (such as student records or personal identifiers), consider encrypting the email or using password-protected attachments to add a layer of security. Encryption or password protection is mandatory when sending student records, grades, or personal identifiers.
- Think before sending: Be cautious with attachments and content. Ensure attachments do not contain more data than intended. Once an email is sent, it cannot be unsent – inappropriate or accidental disclosures via email could constitute a data breach.
- Email security: Protect your email account with a strong password and regularly change your password. Do not click suspicious links or download unexpected attachments, as these can compromise data security. IT may monitor and archive emails to comply with retention requirements and to enhance security, since email records are often needed for audits or legal compliance.

Verbal Communication

When communicating information verbally – whether in person, by phone, or via video meetings – employees should take care to maintain confidentiality and professionalism:

- Private conversations: Discuss sensitive or personal information in a private setting. Avoid conversations about confidential matters in public areas or common spaces where unauthorized people might overhear. For example, do not discuss student grades or personal details in hallways or elevators.
- Verification: When speaking by phone or video call about sensitive matters, verify the identity of the participant if you are not certain (especially if you did not initiate the call or visit). Ensure that no unauthorized individuals are in hearing range on either end of the call.
- Discretion: Even within the office, be mindful of who can hear you. Use offices or meeting rooms for confidential discussions whenever possible. If a conversation is highly sensitive, consider using a lower voice or postponing the discussion to a more secure environment.
- Recording: Do not record conversations or meetings without proper authorization. If a meeting discussing personal data needs to be recorded (e.g., for minutes), obtain consent and ensure the recording is stored securely.

Written documents (physical and digital)

Creating and handling written documents – whether printed or electronic – requires safeguarding to protect data:

- Document creation: When writing documents that include personal or confidential data (such as reports, lists of student marks and names), include only the information necessary for the task at hand. Label documents containing sensitive data as “Confidential” if appropriate.
- Secure storage: Store physical documents with sensitive information in locked cabinets or drawers. Do not leave files containing personal data (like student records or employee details) unattended on desks or in meeting rooms. For digital documents, save them on approved secure storage (such as the organization’s server or cloud storage with access control) rather than on personal devices or unapproved cloud services.

- Limited access: Only share documents with those who are authorized to view the information. If you distribute a report or memo internally, ensure it only goes to the relevant staff. Do not share internal documents with external parties (including students or parents) unless it's part of an authorized process or requirement.
- Safe distribution: When sending documents that contain sensitive data, use secure methods. For example, if emailing a confidential document externally, use encryption or a password-protected file. For internal distribution, ensure the channel (email, internal drive, etc.) is accessible only by intended recipients.
- Proper disposal: When a document (physical or digital) is no longer needed, dispose of it securely. Shred paper documents that contain confidential or personal data – do not throw them in regular trash. For digital files, follow IT guidelines to permanently delete or archive them. This prevents unauthorized access to discarded information.
- Printing: Be cautious when printing documents with sensitive data. Pick up printouts immediately from shared printers.

Internal vs. External Communication

All employees must understand the distinction between internal and external communications and handle information accordingly:

- Internal communications: These include emails, memos, chat messages (e.g., Telegram), and meetings intended for staff or authorized personnel only. Such communications are confidential to the organization. Do not share internal communications with external parties (students, parents, or anyone outside the organization) without approval. For instance, internal staff emails or messages should not be forwarded to students. Breaching this confidentiality undermines trust and could violate privacy regulations. Remember that even within the organization, information should be shared only with those who need to know it.
- External communications: When communicating with external parties (such as students, applicants, parents), ensure that you only disclose information that you are authorized to share. Do not reveal internal discussions, other individuals' personal data, or any confidential internal matter in external communications. All external communications should be professional and comply with both this policy and the organization's public communication guidelines.
- Social media and personal devices: Do not discuss or disclose any confidential work information on social media, personal blogs, or informal channels. Similarly, avoid using personal devices or accounts for communicating work information unless explicitly permitted and secured. Employees using personal devices or unofficial channels to discuss company or student information create compliance risks. Always prefer organization-sanctioned communication tools, which are monitored and secured, to prevent data leaks.
  Secure, university-approved apps (such as Outlook or Teams) are acceptable for use on personal devices, provided they are configured with required security controls.
- Awareness: Be aware that once information is shared outside the organization, we lose control over its distribution.

Best Practices for Data Protection in Communication

To complement the above guidelines, all staff should follow these general best practices derived from industry standards and data protection regulations:

- Data minimization: Share the least amount of personal data necessary for communication. For example, if identifying a student, you might not need to include their full ID or sensitive details in an email when a name or an ID number suffices.
- "Need to Know" basis: Before communicating information, especially personal or sensitive details, consider who truly needs to receive it. Only include those recipients who have a legitimate need for the information. Internally, avoid mass-emailing sensitive information to large groups.
- Secure communication tools: Utilize approved, secure communication platforms provided by the organization. Unsecured channels (personal email, texting apps, etc.) should be avoided for work matters, particularly if they involve personal data, as they are not monitored or protected by our IT Department. Using secure, business-grade tools helps ensure data is encrypted and access is restricted to authorized users.
- Training and awareness: Stay informed through the organization's data protection training programs. All staff should understand how to handle personal data and confidential information. If you are unsure about how to communicate certain information safely, seek guidance rather than guessing.
- Email privacy: Remember that work emails are company property and may be subject to monitoring or legal discovery. Always write emails (and other messages) under the assumption that they could be reviewed by management or, in legal contexts, by regulators. This helps maintain professionalism and compliance.
- Incident reporting: If you suspect that an email or message was sent to an unintended recipient, or if you become aware of any data breach (no matter how minor), report it immediately. Prompt reporting allows the organization to take steps to mitigate any potential harm, and in cases of certain data breaches, legal obligations may require us to notify affected parties or authorities within a short timeframe.

All incidents must be reported immediately, and no later than 24 hours, with escalation to the Academic Registrar and IT Department.

Examples of Acceptable and Unacceptable Practices

Acceptable Practices

- Using your official BMU Outlook account to email students module-related announcement (no personal identifiers beyond name and BMU ID).
- Redacting student addresses before sharing a graduation list with the external events team.
- Forwarding an internal report to the Ministry of Higher Education when formally requested.
- Sharing anonymized survey data with a class for teaching purposes (e.g., percentages instead of raw student names/IDs).
- Using BMU-approved apps (Outlook, Teams) on a secured mobile device with password protection to answer student queries.
- Discussing academic performance with a student only in a private setting (office or one-to-one call).

Unacceptable Practices

- Forwarding staff-only emails (e.g., exam board discussions) directly to students.

- Posting screenshots of grade spreadsheets or internal dashboards in personal chat groups or social media.
- Sending student grade lists via personal Gmail, or Telegram.
- Leaving printouts of student attendance or grades unattended in classrooms or meeting rooms.
- Discussing student disciplinary cases in public spaces (hallways, cafeteria, etc.).
- Including unnecessary details (e.g., full passport numbers, home addresses) in routine internal memos.
- Using personal devices without security controls to store or transmit BMU information.

Compliance and Consequences

Adherence to this Data Protection and Communication Policies is mandatory. The organization takes data protection seriously; failure to comply with these guidelines can result in disciplinary action. Depending on the severity of the violation, consequences may include retraining, formal warnings, or up to termination of employment.

All employees are therefore expected to consistently apply this policy in daily work. Managers and IT personnel will support compliance by providing secure tools, training, and oversight (such as email archiving or audits). Remember that maintaining data privacy and security is not just about avoiding penalties; it is about upholding the trust that students, parents and colleagues place in us to handle their information with care and integrity. By following this policy and best practices, we create a safer communication environment for everyone and protect the organization's mission and reputation.

Revision History

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

Rector: Yuri Loktionov