



24 June 2021

MEMORANDUM CIRCULAR NO. 69

Series of 2021

T O: All VSU Faculty & Staff

R E: Ensuring Data Privacy in the Use of Communication Platforms

At VSU, we value the importance of both communication and privacy. It has been observed that VSU employees use social media and external email platforms to communicate with colleagues about work-related matters. After careful assessment by our privacy compliance officers, we find that this poses a serious risk to the privacy of institutional and personal information that we use at work.

We have invested in official platforms (Google Workspace, Workplace, Zoom, etc) with enhanced or end-to-end encryption so it is fitting for us to use them for communication as we perform our duties.

The university is imposing the following measures to further ensure privacy of our data effective immediately:

1. Internal communication among staff

- a. Sharing of internal work files should only be done through VSU¹ email, Drive, Workplace² and Workplace chat.
- b. Email communication should only be done through the VSU email, not Gmail, Yahoo, or external email service providers.
- c. Synchronous communication among individuals and work groups should be done on Workplace Chat, Zoom, Google Meet, and Discord³ text and voice channels. The use of Messenger for group chats is highly discouraged, also to respect employees who regard the platform as a personal space. Staff without Workplace or Discord may use end-to-end encrypted platforms such as Telegram or Viber.
- d. University updates may be posted in the appropriate groups in Workplace and text channels on the VSU Faculty & Staff Discord Server.
Internal discussions may be done through the abovementioned platforms, like the VSU Town Hall on Workplace.

2. External communication to official partners, students, and other individuals and organizations

¹@vsu.edu.ph institutional account

² Log in to vsuph.workplace.com

³ Join the Server at discord.gg/3r3PZ9Z

- a. Email communication and sharing of work-related files should be done through the VSU email and Drive and not through other email and social media platforms.
- b. Synchronous communication such as group chats are allowed in platforms that are end-to-end encrypted such as Zoom and Telegram. The use of Messenger is highly discouraged. If these platforms are unavoidable, at no instance shall VSU files be shared except via VSU email.
- c. Only share documents and other contents that are for public consumption, such as certain memorandum circulars, advisories, and promotional materials.
- d. For class communication, use VSUEE, Google Meet, Zoom, or Discord. The use of group chats on Messenger is highly discouraged to prevent unauthorized sharing of VSU IMs and other learning materials, as well as to safeguard the faculty's personal space.
- e. Be mindful in submitting personal information to external forms and platforms, especially by non-government agencies.

3. Other platforms


- a. Other platforms not mentioned above should be reviewed by the VSU Web Team and ICTMC before adoption.

I am instructing the **VSU Web Team** and the **ICT Management Center**, in coordination with the Data Protection Officer and Compliance Officers for Privacy, to draft implementing guidelines, design an onboarding program, and monitor to ensure compliance by all VSU units through the Quality Management System.

Administrators of work-related communication in unsecure platforms such as Messenger should immediately initiate moving our users to more secure apps as mentioned above.

Heads of units shall be responsible for the compliance of their unit and staff to the provisions of this memorandum on or before August 2021.

For strict implementation.


EDGARDO E. TULIN
 President

cc: Head, ICT Management Center
 Head, VSU Web Team
 Data Protection Officer
 Compliance Officers for Privacy (Main campus & Component Colleges)
 Director for Quality Assurance
 University DRC