University of the Philippines Diliman
Data Protection Office

upd.edu.ph/privacy
dpo.updiliman@up.edu.ph
(632) 8255-3561

05 May 2020

MEMORANDUM

UPD DPO Memorandum No. EBM 20-05

FOR	:	Deans, Directors, Heads of Units, Faculty, REPS, Staff, Information Officers and Privacy Focal Persons
SUBJECT	:	**UP Diliman Email Policy**

Email is at the heart of work-related connectivity internally and externally.

In line with the UP Diliman Data Protection Officer's responsibility to issue privacy policies under Office of the Chancellor Memorandum No. MLT 19-073, the attached Email Policy is hereby promulgated.

(Sgd.) Elson Manahan
Data Protection Officer

(Sgd.) Regine Estillore
Data Privacy Legal Officer

University of the Philippines Diliman

EMAIL POLICY

The University of the Philippines Diliman recognizes the use of electronic mail (email) as an essential means of communication both within the University of the Philippines Diliman and University of the Philippines System, and externally.

Thus, there is a need to ensure its proper usage and maintain the privacy and confidentiality of information being processed. To this end, this email policy is hereby adopted.

Chapter I. Preliminary Provisions

Section 1. *Scope and Objectives.* – This Email Policy (herein after referred to as "*Policy*") applies to all UP Staff provided with email services managed by or for the University of the Philippines.

This Policy is issued to ensure the proper usage of email and maintain the privacy and confidentiality of information being processed. This includes:

a. Mandatory use of the UP Mail;
b. Establish guidelines to ensure that the use of emails are in line with the mandate of the University; and
c. Adoption of the appropriate security measures to ensure the protection of confidential information, and prevention of data and security breaches, as well as any form of damage to UP Diliman's reputation and technological property

Section 2. *Definition of Terms.* – For the purposes of this Policy, the following definitions shall apply:

a. ***Confidential Information* –** refers to information that is generally non-public data or information by, originating from, pertaining to, under the possession of, owned by, or related to the University of the Philippines Diliman, the University of the Philippines System, UP Constituent Universities, and their respective colleges, offices, units, instrumentalities, and their respective officers, employees, agents and representatives.[1]

   Research work, regardless of its part or stage, including processed and unprocessed data forming part of, in relation to, and arising from such research work, is also deemed as confidential information;[2]

b. ***Personal Information* –**refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained, or when put together with other information

[1] UP Diliman Message and Communication Policy, University of the Philippines Diliman Office of the Chancellor Memorandum No. MLT-18-135, dated 23 May 2018
[2] *See* Note 1

would directly and certainly identify an individual.[3] This is deemed to include sensitive personal information[4] and privileged information.[5]

c. ***Private Information*** **–** refers to personal or confidential information directly or indirectly by, originating from, pertaining to, under the possession of, owned by, or related to the University of the Philippines System, including the University of the Philippines Diliman, and their respective units, personnel and representatives;[6]

d. ***Staff and Faculty*** refers to UP Diliman staff, regardless of rank or employment status, including Research, Extension and Professional Staff and Faculty (REPS), UP contractual personnel, Non-UP contractual personnel, and retirees, as well as UP Diliman Faculty, regardless of rank or employment status, including visiting faculty;

e. ***Units and Offices*** refer to UP Diliman Academic Units and Administrative Offices;

f. ***UP People*** refers to Staff and Faculty, faculty, researchers, alumni, subcontractors, students, outsourcees, agents and representatives of UP Diliman

Chapter II. Mandatory Use of UP Mail

Section 3. ***UP Mail*** **–** UP Diliman has two official email services: UP Mail and UPD Webmail (collectively, "UP Mail"). UP Mail (@up.edu.ph) is an email service available to all currently enrolled UP students and employed faculty and staff (whether regular, or contractual or Individual Contract of Service), and offices. UPD Webmail (@upd), on the other hand is an email service maintained by the UP Diliman Computer Center. The former is used as the official access to the Core Information Systems and standard to all constituent universities (CUs).

In order to promote professionalism and institutional identity, UP People are strongly enjoined to use UP Mail in the conduct of their administrative and academic work. For vital official communications to external parties which related to the official affairs of a UP Diliman unit or office, the use of UP Mail.

The use of personal email is discouraged unless there is an important urgent matter and the user has no access to UP Mail.

---

[3] Sec. 3(g), AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THEGOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES or Republic Act No. 10173 (hereinafter referred to as the Data Privacy Act of 2012 or DPA of 2012).

[4] Sec. 3 (l), R.A. No. 10173 provides that: (l) *Sensitive personal information* refers to personal information:

(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

(4) Specifically established by an executive order or an act of Congress to be kept classified.

[5] Rule I, Sec. 3 (q) defines privileged information as "any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication"

[6] *See* Note 1

Chapter III. Usage and Maintenance

Section 4. *Absence of vested rights* – The use of UP Mail is a privilege, not a right, granted by the University to UP People. As a privilege, UP People have no vested rights over the same.

Section 5. *Legitimate use of UP Mail* – The use of UP Mail shall be for work or academic purposes only. Moreover, its use should not be contrary to law, morals, and public policy.

Furthermore, adherence to the Security Measures laid down in the UP Diliman Privacy Manual[7] as well as UP System's Acceptable Use Policy[8] is mandatory.

When submitting papers to local and international conferences, sending out invitations to UP events, and registering or subscribing to institutions in relation to one's administrative or academic work, UP People are highly enjoined to use the UP Mail.

UP People are to refrain from including as recipients those who have no official business in an email matter. Any unnecessary private or confidential information should be redacted when forwarding an email to others.

Section 6. *Signature* – As part of the effort to maintain the professionalism and proper representation of UP Diliman, UP People are highly encouraged to create an email signature in the suggested format:

[Name]
[Designation]
[Academic Unit/Administrative Office]

Chapter IV. Security Guidelines

Section 7. Access to UP Mail – Access to the UP Mail account shall strictly be made through secured private networks only.

Section 8. *Password or passphrase, and multi-factor authentication* – UP people are required to use a strong password or passphrase. The use of any personal information or common alphanumeric combinations (e.g., password123, QWERTY1111) are prohibited. Passwords, passphrases, and security questions and answers should not be shared with anyone. Passphrases are recommended to be used. Passphrases are a set of words, names or terms which are easy for the user to remember but is difficult for others to guess and too long for computers to crack.

UP People are required to secure their UP Mail accounts using a multi-factor authentication system.

Section 9. *Constant vigilance in accessing links and downloading files* – UP People are expected to exercise constant vigilance in using their UP Mail accounts. They are expected to be wary of phishing and malware attempts and exercise caution in downloading files. Only the

[7] Chapter IV, Data Protection Team Memorandum Reference No. EBM 19-02, dated 11 November 2019
[8] *See* Note 6

files that are necessary in the conduct of their official and/or academic work may be downloaded.

Moreover, UP People are to refrain from accessing links or opening emails from unidentified or unfamiliar senders. Clickbait subject headings or links, suspicious emails or those containing inconsistencies such as grammar mistakes, excessive punctuation marks, requesting for donations, should likewise raise caution. In case of doubt, the UP Diliman Computer Center may be consulted.

Before downloading an attached file, the user must: first, ensure that it is from a recognized and legitimate source; and second, scan for any viruses or other threats.

Section 10. ***Prevention from unauthorized access and/or use*** **–** In order to prevent any unauthorized access and/or use of one's UP Mail account, only the registered account holder shall be authorized to use his/her UP Mail account.

Section 11. Security Breach – In the event of a security breach, such as, but not limited to hacking, the UP Mail account holder should immediately inform the UP Diliman Computer Center.

Chapter V. Confidentiality of Information

Section 12. ***Compliance with the UP Diliman Message and Communications Policy*** **–** The creation, sending, transmittal, receipt, and storage of emails should be inline with the UP Diliman Message and Communications Policy.[9]

Section 13. ***Exercise of due diligence in processing private information*** **–** UP People are expected to exercise due diligence when processing Private Information through email.

In case of doubt, all emails shall presumed private and confidential.

Section 14. ***Confidentiality of private information*** **–** Private Information contained and processed in emails are strictly confidential and are deemed to be strictly for the sender and recipient's use only.[10]

Section 15. ***Reproduction, transmittal, etc. of private information*** **–** No part of the email containing or pertaining to Private Information shall be reproduced, transmitted, or exhibited in any form or manner without the written consent of the sender and the University. However, the consent of the University does not amount to the consent of the data subject, intellectual property owner, or the original source of the Private Information.[11]

Section 16. ***Transfer of data*** **–** To ensure the security and privacy of personal information, users must ensure that the data is encrypted, or sent through a facility that facilitates the encryption of data, including its attachments.[12]

Section 17. ***Privacy and confidentiality notice*** **–** Official communications through email containing or referring to Private Information shall contain a Privacy and Confidentiality Notice placed at the end of the email (footer).

[9] *See* Note 1.
[10] Ibid.
[11] Ibid.
[12] National Privacy Commission Circular No. 16-01, Security of Personal Data in Government Agencies, dated 10 October 2016

Below ae the sample wordings for a Privacy and Confidentiality Notice:[13]

a. English:

Privacy and Confidentiality Notice

This message, its thread, and any attachments are privileged and confidential. No part of this message may be reproduced or exhibited in any form or manner without the consents of the sender and the University of the Philippines Diliman. In case of wrongful receipt of or unauthorized access to this message, please immediately inform the sender and permanently delete all wrongfully received copies. Your access to this message subjects you to the UP Diliman Message and Communication Policy and relevant data privacy regulations

b. Filipino

Pabatid sa Pribasiya at Pagiging Kumpidensiyal

Ang mensaheng ito, kasama ang mga karugtong, at anumang mga kalakip ay pribado at kumpidensiyal. Maliban sa tunay na layunin ng mensahe, walang bahagi nito o identidad ng tao ang maaaring ibunyag, kopyahin o ipalabas nang walang pahintulot mula sa nagpadala. Kung di-sadyang natanggap o nabasa ang mensaheng ito nang walang pahintulot, agad na ipagbigay-alam sa nagpadala at permanenteng burahin ang lahat ng di-sadyang natanggap na kopya. Ang iyong pag-akses sa mensaheng ito ay nangangahulugang sumasailalim ka sa UP Diliman Message and Communication Policy at anumang kaugnay na mga tuntunin ukol sa pribasiya ng datos.

The aforementioned footers are suggested wordings for the Privacy and Confidentiality Notice. The contents of the same may be revised in accordance to the context of each correspondence.[14]

In determining whether such Notice must be placed the following requisites must be complied with, to wit:

a. The message is an official message from the University;
b. The message contains confidential, privileged, or personal information; and
c. The message is from the University of the Philippines System (including UP Diliman), and the recipient is a non-UP party.

The absence of any of the foregoing, the placement of such Notice is not required.

The University of the Philippines System is deemed as a single juridical entity. Consequently, all the emails within the University of the Philippines System are considered as internal in nature. Therefore, there is no disclosure to third parties to speak of when the email is from one UP unit/office to another.[15]

[13] *See* Note 1

[14] *See* Note 1

[15] Clarifications on Privacy and Confidentiality, Non-Disclosure Agreement, and CCTV Notice, Office of the Chancellor Memorandum No. MLT 19-113, dated 25 March 2019

Corollary thereto, if the email is from a UP Diliman administrative office or academic unit, sent to an external party, (e.g., OVCAA sends an email to the Bureau of Internal Revenue), then a Privacy and Confidentiality Notice must be placed at the end of the email.

However, it must be noted that internal and personal messages from one UP staff and faculty to another is not covered by the University's Privacy and Confidentiality Policy.

Section 17. *Sensitive confidential information* – Whenever sending an email containing sensitive confidential information, the following notice must be placed as a header:

> This email contains **Sensitive Confidential Information** under the UP Diliman Data Classification Policy. As such, the contents of this email *may only be disclosed on a need-to-know basis* to the minimum number of University of the Philippines officials and staff who are highly necessary to resolve the issues in this email.

Under the UP Diliman Data Classification Policy, sensitive confidential information refers to information that may likely cause serious harm to UP Diliman or other individuals if not strictly protected. This type of information may contain sensitive personal information and privileged information.[16]

Section 18. *Wrongfully received emails* – Any email containing Private Information wrongfully received or accessed without authority should be immediately deleted and disposed of. Furthermore, the University and the sender of the Private Information wrongfully received or accessed without authority should immediately be informed.[17]

[16] UP Diliman Data Classification Policy, Data Protection Office Memorandum No. EBM 19-03, dated 02 January 2020

[17] *See* Note 1