L-Università ta' Malta

Data Protection Office

Policy regarding the Protection of Personal Data in Email and Electronic Communications

Version 1.0

I. Introduction

(a) Staff members and officials of the University of Malta (the 'University' or 'UM') send countless emails daily in the exercise of their functions, roles and responsibilities. Such emails include personal data in the form of recipients' email addresses, and may include other personal data inherent in the text of the emails themselves and/or attached thereto as or in an attachment.

(b) The University is conscious of its obligations under all applicable data protection laws, including the GDPR (Regulation (EU) 2016/679) and the Data Protection Act (Chapter 586, Laws of Malta), is aware that unintended and/or unauthorised disclosure of the above-mentioned personal data gives rise to adverse consequences for both the individuals whose personal data has been disclosed and for UM itself, and is committed to processing such data in a manner that complies with the applicable laws.

II. Purpose

(a) This Policy sets out overarching principles intended to protect the privacy of personal data included and/or inherent in emails and attachments sent by UM staff members and officials and the rights and freedoms of the individuals to whom such data pertains.

(b) This Policy shall be supplemented by internal entity-specific sub-policies (the 'Sub-Policies') detailing the procedures to be followed by UM entities to implement the principles set out herein.

(c) It shall be the responsibility of UM entities to establish a Sub-Policy as afore-mentioned after determining the best manner of implementing the principles set out in this Policy that is conducive to their operations. This Policy should thus serve as a foundation for such Sub-Policies.

III. Scope

This Policy applies to all UM staff members and officials.

IV. Policy Statements

(a) This Policy governs:

(i) the sending of emails to UM students, UM alumni, external recipients and to a large number of recipients;

(ii) the inclusion of a disclaimer in outgoing emails; and

(iii) the sharing of attachments.

Emails to UM students and UM alumni

Emails to UM students and UM alumni should be sent without revealing the identity and/or email address of the students or alumni on the corresponding distribution list.

Emails to external recipients

Emails to external recipients should be sent without revealing the identity and/or email address of the individuals on the corresponding distribution list.

In select instances, emails to a small number of external recipients who know each other may be sent in a manner which permits the identification of such recipients. For instance, an email about a project or initiative which the University is pursuing with an external entity to the staff members or officials of such entity who are also working on the said collaboration need not be sent without revealing the identity and/or email address of the individuals on the corresponding distribution list.

Emails to a large number of recipients

Emails to a large number of recipients, whether internal or external, should be sent without revealing the identity and/or email address of the individuals on the corresponding distribution list.

Disclaimer

The following disclaimer shall be added to all outgoing emails sent, and/or attachments shared, by UM staff members and officials:

This message, its contents and any attachments thereto are intended solely for authorised recipients and contain information that is or may be confidential and/or that is or may also be privileged or otherwise exempt from disclosure. Any use, disclosure or reproduction of this message and/or its contents without the sender’s express consent is strictly prohibited and may be unlawful. If you have received this message in error, please inform the sender immediately and delete it from your system.

Sharing of attachments

(a) Attachments should be shared in a secure manner that prevents or limits to the greatest extent possible the disclosure of such documents to unauthorised recipients. In lieu of by email, alternative secure means of sharing attachments should be explored and implemented. Attachments should only be sent by email as a last resort.

(b) UM staff members and officials shall, prior to sending outgoing emails and/or to sharing attachments, double check that the recipients of such correspondence, and/or that any documents to be shared, are the correct and intended ones. This manual checking shall be without prejudice to any technical and/or overarching measures that may be introduced by UM to enable and/or facilitate additional checking of emails sent and/or attachments shared.

(c) In cases of doubt, the advice of the UM Data Protection Officer should be sought prior to the sending of any email and/or the sharing of any attachment.

V. Responsibilities

(a) The Data Protection Office is the owner of this Policy.

(b) UM entities are responsible to establish their own Sub-Policies detailing the procedures they will follow to implement the principles set out in this Policy within three months of the coming into force of this Policy, and shall, in doing so, use this Policy as a foundation.

(c) IT Services shall provide technical guidance as and when requested by UM entities establishing the afore-mentioned internal policies, to enable such entities to determine and establish the best manner to adhere to the principles set out in this Policy.

(d) UM staff members and officials are responsible to:

(i) Abide by the principles set out in this Policy and by the corresponding procedures and principles set out in their entity-specific Sub-Policies; and

(ii) Report any unintended and/or unauthorised disclosures of personal data by email to the Data Protection Officer immediately upon becoming aware of such disclosure, on dpo@um.edu.mt or +2340 3233.

VI. Breach of Policy

Breach of and/or failure to adhere to this Policy may lead to disciplinary action.

Approved by Council on 27 September 2019.