



## GENERAL POLICY FOR THE USE OF ELECTRONIC COMMUNICATIONS AT THE PONTIFICIAL CATHOLIC UNIVERSITY OF PUERTO RICO



### I. Introduction

#### A. Justification

According with the use of technological resources as means of communication, the Pontifical Catholic University of Puerto Rico (hereinafter *University* or PCUPR) recognizes the need to establish regulations for their proper use. The University also recognizes that electronic communication mechanisms are very effective and far-reaching. For this reason, the responsible use of these resources is essential to adequately meet institutional objectives; and have an effective mechanism to keep the university community and the rest of the world informed.

#### B. Objectives

The General Policy for the Use of Electronic Communications at the Pontifical Catholic University of Puerto Rico aims to provide principles, rules, and procedures for the efficient, effective, and secure use of the digital means of communication used to exchange or publish information. This includes electronic mail (email), instant messaging services (chats), institutional electronic forums, discussion groups and videoconferences.

#### C. Scope

The General Policy for the Use of Electronic Communications at the Pontifical Catholic University of Puerto Rico applies to all users of electronic communication systems, understood as professors, students, non-teaching staff and any person who has access to said resources (hereinafter *Users*). This policy also applies to external persons who provide or receive any service at the University. Applies to all electronic communication resources (Moodle, Zoom and the Pioneer Access Portal) that belong to or are managed by the Pontifical Catholic University of Puerto Rico, or other resources provided by the University through contracts or agreements.

#### D. Google Apps for Education

The service known as Google Apps for Education (GAE) is the primary electronic communication system of the university community. This platform provides an account

that allows users to access institutional email services, calendar, instant messaging, videoconferencing and information storage. Therefore, in order to optimize official communications sent to the entire university community or to sectors of it, it will be understood that the email account accessed through the GAE is the official institutional email account. For the purposes of the Pontifical Catholic University of Puerto Rico, all official email accounts must have the domain **@pucpr.edu**.

## **II. Usage Policy**

### **A. Acceptance of the conditions and rules of use**

The use of the email service and other means of electronic communication provided by the University implies, on the part of the Users, the knowledge and full acceptance of the rules of use and conditions that are specified in this section and in all the documents complementary acceptable use of PUCPR information resources and technologies.

### **B. Confidentiality of Electronic Communication Media Access Accounts**

Each user will be assigned an account that will contain two elements: username and password. The user is responsible for maintaining the confidentiality of his password and all activities carried out from it.

### **C. Exclusive use of institutional email for professional or academic purposes**

Institutional email is recognized as an official method of exchanging information. As official electronic documents, any official transaction, document or communication using email is expected to use an official email account. Users must not use or refer to email accounts external to the University to carry out official electronic communications.

The PCUPR email is a tool for the exchange of information related to the user's work or study tasks. It is not a means of mass and indiscriminate dissemination of information.

### **D. Exclusive use of other means of electronic communication for professional or academic purposes**

Instant messaging and video conferencing are recognized as official means of exchanging information. It is expected that any management, document or official communication using instant messaging and videoconferencing uses an official email account of the University. No use or reference should be made to external access accounts to the University to carry out official electronic communications.

Instant messaging and videoconferencing are tools for exchanging information related to the user's work or study tasks; it is not a means of mass and indiscriminate dissemination of information.

Institutional accounts for instant messaging and video conferencing should not be used for personal use.

#### **E. Privacy Expectation**

The University recognizes and respects the reasonable expectation of privacy of Users regarding their files and electronic communications, to the extent that they are reasonably related to their duties and responsibilities to the University and their content is not prohibited by law or internal regulations. In that sense, in extraordinary circumstances in which there is an imminent danger to the personal integrity of the information or of any person; there is an imminent threat to the safety of one or more members of the university community; or there is reasonable and well-founded suspicion about the commission of conduct prohibited by law or by internal regulations, the President or one of the Vice Presidents of the University may authorize access, review and monitoring of institutional accounts for the use of Google services. Apps for Education provided to members of the university community. Only in such circumstances, the President or any of the Vice Presidents may authorize access to the institutional account of Google Apps for Education of a User to read, block or delete information, subject to the limits provided by the legislation applicable to the preservation of documentary evidence or evidence. Such authorization must be sent in writing to the Executive Director of Telecommunications and Information Technologies, who will order and/or execute the corresponding action, will document the reasons that justify such intervention and will notify the President that the ordered actions have been completed.

#### **F. Prohibited use of official means of electronic communication**

Official means of electronic communication will not be used to:

1. Purposes that are not administrative, academic or research.
2. Sending or replying to chain letters or any other *pyramid* scheme of messages.
3. Business purposes.
4. Send viruses or programs of malicious use.
5. Read third-party communications or generate and/or send messages on behalf of another person, impersonating them or modifying the content of electronic communications previously sent by another person.
6. The distribution or installation of software without the use license acquired by the University (*pirate* software).
7. The distribution and use of books, photos, videos, articles and other materials and documents that violate intellectual property rights (copyright).

8. Introduce malicious software on the network or servers (viruses, worms, spam email blasts, and others).
9. Reveal your username and password.
10. Carry out any type of harassment, defamation, slander, intimidation, insult or any other form of hostile activity.
11. Make fraudulent offers of products or services whose origin is the University's own resources or services.
12. Carry out activities that contravene the security of the systems or that generate interruptions of the Network. These include accessing data addressed to a third party, accessing an application or a server without authorization.
13. Use programs or send messages with the purpose of interfering or adversely affecting the operation of the University Network.
14. Send unsolicited email messages (*spam*).

### **III. Misuse and Disciplinary Actions**

Users are required to report in writing to the Executive Director of the Office of Telecommunications and Information Technologies ([director\\_tti@pucpr.edu](mailto:director_tti@pucpr.edu)) the improper use of official means of electronic communication to avoid its repetition or repercussions to other users. Any violation of this Policy is subject to legal consequences as they arise from state or federal legislation and/or disciplinary sanctions as established by University regulations.

### **IV. Best Practices**

The PCUPR has an informative page where some of the best practices are exposed to minimize potential risks associated with communications and information systems. This page can be accessed at <http://www.pucpr.edu/seguridaddelainformacion/>.

### **V. Amendments**

This Policy may be amended, from time to time, by the Administrative Board of the PCUPR, which will notify the users of the changes adopted by the media it deems appropriate.

This policy was approved by the Administrative Board on February 16, 2017.