Electronic mail is used today by people everywhere to share and transmit various information. Its usefulness, notwithstanding, the email’s popularity as a communication tool also makes it a common target for hackers and other parties who exploit its vulnerabilities to perpetrate fraud and other criminal activities. At the same time, its reckless use makes it highly susceptible to data breaches and other security incidents.

Here are some reminders.
ADVISORY NO. 18-01
Email Use and Data Protection

Background

Facilitated by the advent of the Internet era, electronic mail or "email" is used today by people everywhere to share and transmit various information (e.g., personal data). They include those working within the context of schools and academic institutions.

Its usefulness, notwithstanding, the email’s popularity as a communication tool also makes it a common target for hackers and other parties who exploit its vulnerabilities to perpetrate fraud and other criminal activities. At the same time, the reckless use of the medium makes it highly susceptible to data breaches and other security incidents.

This has compelled governments and other stakeholders to develop information security and data protection policies designed to lower the prevalence of email-related crimes and data leaks.

Here in the Philippines, Republic Act No. 10173, or the Data Privacy Act of 2012 (DPA), is one such policy. The law provides for the protection of personal data by establishing principles that govern data processing, and imposing requirements such as the implementation of organizational, physical, and technical security measures.

In line with the provisions of the DPA, the Ateneo de Manila University has established the University Data Protection Office (UDPO) to ensure the school’s compliance with the law, via the creation of a comprehensive data protection framework. A key component of this framework is the development and implementation of policies and guidelines that assist University units and their respective personnel in aligning their processes and activities with the tenets of the DPA.

The UDPO now issues these guidelines on the proper conduct of email communications using official or University-issued email accounts.

Scope

This Advisory covers all offices and individuals who use an official or University-issued email address (i.e., @ateneo.edu) by reason of their affiliation, engagement, or relationship with the Ateneo de Manila University.
Guidelines

1. **Use your official email account in work-related communications**

   It is prudent to use the email account issued to you by the University when communicating in relation to your work for or in the University, for a number of reasons:

   - It lessens the chances of you unnecessarily disseminating private and/or confidential information to unintended recipients by having your work-related messages separated from private correspondences.
   - It allows you to benefit from any or all technical security measures that have been put in place by the University to protect its information technology (IT) resources.
   - It lets you enjoy more privacy by making it difficult for other people to locate you through your social media account/s and other online services you have signed up for. When you establish a social media account (e.g., Facebook, Twitter, Instagram, etc.) or avail of online services (e.g., forums, games, surveys, etc.), you are often required to register by identifying your email address. Many of them allow their users to look for friends or acquaintances by inputting the latter’s email addresses.

2. **Minimize the use of your official email account in your personal or household affairs**

   Conversely, it is best to avoid using your University-issued email account in matters that are not related to your work for or in the University in order to avoid, among others, dangerous, malicious, or unsolicited messages. This usually means you should not disclose your official email address during activities you perform, attend, or join in your personal capacity, such as:

   - opening social media accounts
   - using desktop or mobile applications and other online services
   - attending events, conferences, or seminars
   - joining contests, competitions, or raffles
   - subscribing to magazines, newsletters, or promotional materials

   Granted, there are instances when a school-affiliated (i.e., .edu) email account is useful when availing of certain online services. While this is permissible, you should always exercise discretion and check if you are dealing with a reputable organization or company in order to keep your official email address from fraudsters and other shady individuals. At the very least, read first the entity’s Privacy Policy or Terms and Conditions.

3. **Be careful when opening or receiving emails, especially from unknown or unfamiliar sources**

   It is common for hackers and other criminals to defraud unsuspecting individuals or compromise the computer systems of companies using emails as an entry point. For this reason, one has to be extra careful when receiving and opening them, especially when unexpected or coming from unknown sources. To exercise caution:

   - Check if the email address of the sender is legitimate. Malicious emails are sometimes made to look like they are coming from legitimate or familiar sources. The sender often does this by replacing some characters or portions of the email address. (e.g., “@1nquirer.com” instead of “@inquirer.com”, “@mobile.tv” instead of “@mobile.com”, etc.)
• Verify any suspicious claim or statement in the email. Sometimes criminals hijack or gain access to the email account of your acquaintance, friend, or relative, and then use the same to solicit money or information from or about you.

• Do not click on links embedded in emails, especially when the message is from an unknown source. Sometimes, all it takes for the sender to gain access to your computer is for you to click on those links. Maintain this same level of caution even if the message appears to be coming from a legitimate source (e.g., your bank, your social media account, your email provider, etc.).

• Similarly, do not open any attachments to an email you are not expecting to receive, or if coming from an unknown source. Many viruses and malicious software are activated as soon as the files containing them are opened. If you have an anti-virus software, it is always advisable to scan any or all email attachments before opening them.

• If possible, avoid altogether opening emails that are unsolicited or patently malicious. Opening such emails already exposes you to some harm, or will at least leak information about you to the sender and other third parties. If an email contains a tracking client, as soon as you open it, the sender may be informed of one or all of the following: (a) that the email has been opened—which means your email account is still active; (b) your IP address, and therefore your location or workplace; (c) the device you used to open the email; (d) your schedule—based on the time you check your email; (e) your itinerary—based on how you check your emails; and (f) personal preferences—based on where the sender harvested the email address, say, a sports forum, or a music fansite.

4. Do not draft emails while distracted

Always maintain focus when drafting an email, especially when the message contains sensitive or confidential information. While many people claim to be adept at multi-tasking, writing an important communication requires one’s full, undivided attention. There are plenty of examples of data breaches caused by distracted individuals who ended up sending unfinished messages, attaching wrong files, and/or indicating the wrong recipients.

5. Avoid discussing sensitive or confidential information via email threads, while limiting discussions regarding personal data, in general

To the extent possible, refrain from discussing sensitive or confidential matters on email threads, and keep any discussion regarding personal data to a minimum. This is particularly true when a thread involves multiple recipients who may have different levels of authorization or access to certain types of information.

6. Draft your subject line properly

Make your subject line short but accurate. If possible, refrain from including personal or sensitive details in the subject line. When appropriate, mark your subject as ‘Private,’ ‘Confidential,’ or ‘ Classified,’ enclosed in brackets; but be sure to complement this measure by putting the private, confidential, or classified information in an attached file that is password-protected or encrypted.

7. Limit the disclosure or sharing of personal data, whenever possible

While proper spelling, grammar, and punctuation are a given when writing emails, you should also pay attention to the information you disclose or share in them. The proportionality principle
in data protection demands that you only process (i.e., disclose) the minimum amount of information necessary to achieve or accomplish the purpose of your data processing. In other words, relay your message effectively without disclosing too much information.

8. **Make sure you have the correct attachment/s**

If you need to attach one or more files/documents to effectively communicate your message, make sure that the correct document/s are attached. Otherwise, it may result in the unintentional sharing or disclosure of personal data, which almost always qualifies as a data breach. In some cases, this also means checking if: (a) all pages of a particular document actually need to be shared; or (b) one or more items in the document needs to be redacted, covered, or removed.

9. **Whenever appropriate, make sure your attachment is password-protected**

If your email attachments contain sensitive and/or confidential information, limiting access to them using password protection is recommended. That way, in the unlikely event that the email is missent or opened by an unauthorized person, the unintended recipient will be unable to open the attachments without additional tools or technical proficiency. Most document processing software available today now have this feature. To inform the intended recipient of the password, you may do so in person or via other means (e.g., phone call, text message, etc.).

10. **Add the email address of the recipient last**

As a general rule, always add the email address of your intended recipient last when drafting a message. This helps avoid the sending of an incomplete or unfinished email—one that has not been proofread, or one that is lacking the necessary attachment.

11. **Use the CC and BCC features responsibly and sparingly**

Do not be quick to add recipients on the “CC” and “BCC” fields. If a person really needs to receive an email, then he/she should be a direct recipient, with his/her email address placed in the “TO” field. The “CC” (carbon copy) field is meant for those who need to be informed of the content of an email, but are not required to take any action. This feature is useful in instances such as when a supervisor wants to monitor how a staff member replies to queries sent to the office. The “BCC” (blind carbon copy) field, on the other hand, is used for sending messages to individuals who do not need to see the other addressees. This is useful for broadcasting announcements to a large group of people. It is also meant to prevent any of the recipients from building an email database that may later be used for improper or illegal purposes.

12. **Make sure you have the correct recipient/s**

Check carefully whether you are sending your message to the correct or intended recipient. This includes making sure there are no typographical or spelling errors in writing down the email address of the recipient. Pay extra attention when your email platform has an auto-complete feature, since a common name could lead to 2 or more different email addresses. If you are not careful, the wrong addressee may be indicated as recipient of your email.

13. **When replying, use the “Reply all” function with discretion**

First of all, check if the email you just received has other recipients. If so, use the “reply all” function only when it is absolutely necessary in order to avoid accidental disclosures of personal
data and other confidential information. To go about doing this, ask yourself the following questions: Do all of the addressees need to be informed of my response? Would replying to only one person suffice? If not, would removing certain people be appropriate?

14. **Use free encryption tools when necessary and whenever possible**

For those handling very sensitive and classified information, encrypting and authenticating individual messages is always an option. Simple, user-friendly, and portable public key encryption programs are available online and can encrypt email messages and files even when you are not connected to the internet.

Following all these recommendations will not offer absolute protection against hacking incidents or data breaches. No amount of precaution can do that. This is true for any security system. There will always be individuals or groups who will find their way into other people’s accounts and data, if they are determined enough and are equipped with the requisite expertise and resources. Also, all it takes is one mistake or one moment of vulnerability, and even the most cautious person can unwittingly compromise sensitive or confidential information by his actions or inaction.

Nevertheless, failure to heed these guidelines will certainly increase significantly the likelihood of you or your office experiencing a security incident or data breach. While most such incidents may only merit a reprimand or admonition from your supervisor or the University, the worst of the lot can lead to serious consequences that are actually punishable under University policies or the law.

Should you have questions or require further guidance regarding this Advisory or any of these recommendations, you may contact the UDPO at info.udpo@ateneo.edu.

For your guidance.

Sgd.

JAMAI EL A. JACOB
Director

Noted by:

Sgd.

JOSE RAMON T. VILLARIN, S.J.
President