ADDITIONAL GUIDELINES ON WORK-FROM-HOME CONDUCT

1. OBJECTIVES:

This is aimed to provide additional guidelines for employees on a work-from-home arrangement. Infractions committed while on work-from-home arrangement shall be treated as having been committed as an employee of the University on official duty or during official activities of the University outside of the campus.

Please be reminded that all employees are expected to act with integrity and good judgement at all times, even when one is working from home. All applicable provisions of the Employee Code of Discipline, Staff Rules and Regulations, and University Code of Conduct and Ethics, as well as other University policies pertaining to employee conduct, such as the Social Media Guide of June 2020 and the UDPO Advisory No. 18-01 on E-mail Use and Data Protection, shall remain in force and effect even when on a work-from-home arrangement.

2. ADDITIONAL GUIDELINES:

2.1 Equipment

Employees are expected to protect from damage or theft the issued/loaned equipment of the University. The issued/loaned equipment shall be used for work-related purposes only, and may not be used by unauthorized individuals or for any other purpose.

2.2 Security

Employees are expected to ensure the protection and security of work data and information that are accessed off-campus. All work documents must be secured in locked file cabinets and desk/s after daily use, sensitive/confidential documents must be password protected especially when sent as attachments to e-mails, and other appropriate security measures must be installed.

2.3 Time Worked

Employees who are entitled to overtime pay are required to accurately record all hours worked following the University's timekeeping standards.

Hours to be worked in excess of those scheduled per day and per workweek require the **advance written authorization** of the employee's supervisor.

2.4 ONLINE CONDUCT

Employees are expected to uphold and protect the University's values and shall not act in any way that may tarnish the University's reputation. They are expected to exhibit good conduct, whether for professional or personal matters, when using online platforms. They are responsible for ensuring that they use the online platforms in an ethical, respectful, professional, responsible and lawful manner.

Please be reminded of the following when using the online platforms for **work-related purposes**:

1. Do not access confidential/sensitive information in an unsecure location.

2. Access information/data only for those you have authorization. I

    a. If you are unsure of the level of your authority to access certain information/data, seek permission in writing from your immediate supervisor and the authorized data controller from your office to access the specific information/data. State clearly the purpose of accessing the same.

       Should the supervisor and the authorized data controller grant persmission to access certain information/data, your access to such shall only be limited to the purpose stated when you sought permission for its access.

    b. If you receive information sent to you through e-mail or other online modes by mistake, contact the sender immediately and permanently delete the information from your system.

3. Secure the consent of all participants prior to audio/video-recording online meetings.

4. Send confidential and sensitive information to authorized recipients only through secure channels.

Please be reminded of the following when using **social media platforms:**

1. Explicitly articulate that your personal statements are exclusively your own and they do not in any way represent the stand of the University if you are identifiable as an employee of the University.

2. Refrain from issuing/posting/sharing discriminatory, derogatory, offensive, defamatory or unlawful statements and content. Present work-related complaints/statements together with evidence to proper channels/authorities as indicated in the Employee Code of Discipline.

3. The privacy policies of the University apply at all times. Do not publish personal or proprietary information, whether via public post or private message, without explicit permission from the owner. Always secure written permission or consent from: (a) a parent or a legal guardian when dealing with information concerning minors, and (b) vulnerable persons.[1]

[1] Vulnerable Person refers to a person of eighteen (18) years of age or over who meets one or more of the following criteria:

- Has a learning or physical disability;
- Has a physical or mental illness, chronic or otherwise;
- Has a mental health condition, including an addiction to alcohol, drugs, etc.;
- Has a reduction in physical or mental capacity;
- Is receiving any form of healthcare;
- Is detained in custody, or is receiving community services because of age, health or disability;
- Is living in a sheltered or residential care home; or
- Is unable, for any other reason, to protect themselves against significant harm or exploitation.

Persons are regarded as vulnerable if they are in "an infirm state, of physical or mental deficiency, or deprivation of personal freedom, that in fact, even occasionally, limits their capacity to intend or to want or in any way to resist the offense."

Students above 18 years of age who are under the supervision of a teacher or other adults in the place of a parent (*principle of loco parentis*) may still be considered vulnerable persons.

4. Refrain from posting on any social media channel any memorandum or document that bears an image of a handwritten signature or signature in wet ink. If in doubt, seek advice from the University Marketing and Communications Office (UMCO), University Data Protection Office (UDPO), or the University Legal and Compliance Office (ULCO).

Vulnerable persons also include senior citizens, the elderly Jesuits living in the Ateneo de Manila campus, and retirees who have requested or have been invited back to the Ateneo de Manila to teach or render service.

References:

1. Employee Code of Discipline https://www.ateneo.edu/code-of-discipline
2. Staff Rules and Regulations https://www.ateneo.edu/staff-rules-and-regulations
3. University Code of Conduct and Ethics https://www.ateneo.edu/ohrmod-policies
4. Social Media Guide of June 2020 http://ateneo.edu/sites/default/files/2020-06%20Social%20Media%20Guide.pdf
5. University Data Protection Office Advisory No. 18-01 https://ateneo.edu/udpo/issuances/advisories