SPU Manila INTER-OFFICE BULLETIN

Vol. XIV No. 13 **19 October 2020**

A WORLD IN CRISIS: COVID-19: PART THIRTY-TWO

And so, the pandemic goes on and on. And so, Metro Manila has been retained on General Community Quarantine until 31 October. And the numbers keep increasing and increasing:

COVID-19 CORONAVIRUS PANDEMIC

Last updated: October 12, 2020	Last updated: October 19, 2020
Coronavirus Cases: 37,739,543	Coronavirus Cases: 40,278,169
Deaths: 1,081,402	Deaths: 1,118,320
Recovered: 28,345,710	Recovered: 30,112,171

The top five countries most affected by the coronavirus are:

	October 12, 2020-October 19, 2020		
	Confirmed Cases	Deaths	Recovered
USA	7,991,998-8,387,799	219,695-224,730	5,128,162-5,457,684
India	7,119,300-7,548,238	109,184-114,642	6,146,427-6,659,895
Brazil	5,094,979-5,235,344	150,506-153,905	4,470,165-4,650,030
Russia	1,298,718-1,399,334	22,597-24,187	1,020,442-1,070,576
Argentina	989,680	26,267	803,965

It will be noted that Argentina has seen an upsurge in cases and is now in fifth place.

In the Philippines, these are the figures:

October 12, 2000-October 19,2020		
Confirmed Cases	Deaths	Recovered
339,341-356,618	6,321-6,652	293,075-310,158

SPU MANILA RESPONSE TO THE PANDEMIC

The St. Paul University Manila Data Protection Office has issued the following guidelines on online communication during this time of the pandemic.

ARE WE SAFE IN AN ONLINE WORLD?

As everybody is using an online mode of sending communication, sharing information, learning, and working, it is very important to know if you are safe or are you putting yourself at risk. Here are some tips for your safety online.

WHILE WORKING FROM HOME

1. Create a strong and memorable password.
    - Think of a memorable password phrase or word containing more than six letters. Example: "privacy"
    - Add a set of numbers at the end to make it even harder to crack. Example: "privacy2020"
    - Replace letters in the word with numbers. Example: "pr1vacy2020"
    - When asked to create a password for a new site, add a first or last letter to match the first letter of the website you are on and make it a capital letter. Example for Google password: "Gpr1vacy2020" or "privacy2020G"
    - Always mix numbers, capitals, and letters. Decide on a formula that works for you, and remember that a phrase is harder to crack than just one word. Example: "Pr1vacY2020"
2. Avoid hiding your passwords:
    - Under your keyboard
    - Under your phone
    - On your monitor
    - Under your mouse pad
    - In your top drawer
    - Under your desk
3. Do not share office account or personal password for:
    - Accountability issues
    - Possibility of undue intrusion, interference, or access to confidential records
    - Distortion/destruction
    - Vulnerability of your private affairs
4. Require the client to present competent proof of identity (for emailed issues).
    - A government ID bearing the photo and signature of the individual
    - School ID for students
    - Not a "sedula" or community tax certificate
    - Official school email account
5. Require proper authorization (if asking for personal information).
    - Except for parents of minors and children of school age
    - Ideally a Power of Attorney
6. Answer inquiries by telephone prudently.
    - Do not give personal information over the phone. The caller's identity is always difficult to verify.
    - Answer only general questions.
7. Send files online after double checking:
    - The content of the file to be sent
    - The email address of the receiving party
    - The legitimacy of the purpose of the request
    - The capacity of the receiving party

8. Do not allow unauthorized background checks.
    - Do not post personal information on online public spaces without consent. Example: grades, addresses, etc.
9. Express your ideas as your own.
    - Do not speak on behalf of your employer, when not authorized. Your employer also has privacy and other rights.
10. Collaborate from home carefully.
    - Be prudent in using group chats. There is no such a thing as a private group chat.
    - Handle confidential data carefully.
11. Create a good working environment.
    - As no one knows how long the pandemic situation is going to last, it is a good idea to create a comfortable working environment for yourself.
    - An organized workspace is not only comfortable but manageable.

WHILE CONFERENCING FROM HOME

1. Do not share virtual meeting details.
    - Avoid zoom bombing.
2. Be discreet.
    - If possible, do not share highly confidential information or data.
    - To protect personal privacy, mute yourself.
    - Use your camera with prudence.
    - Use "official background" because others may make "memes" from your video screenshots.
    - Do not post screen grabs of online meetings without everyone's permission.
    - Share only what you want to be made public.
    - Disable cookies.
    - Go incognito.
    - Clear history.
    - Always logout.

WHILE WORKING FROM "A SHARED SPACE" SUCH AS INTERNET CAFÉ/COMPUTERS/PREMISES

- Avoid "public viewing" of your computer screen.
- Do not let others view school records, which are sensitive personal information.
- Use portable hard drives/thumb drives.
- Avoid saving files in a non-secured or shared computer, which others may conveniently access and even copy.

USING ANTIVIRUS SOFTWARE

- Prevent malware from compromising your personal files, your work, and your employer's systems.

DEALING WITH SUSPICIOUS EMAILS AND WEBSITES

- Accessing malicious websites and emails can compromise your privacy and that of others.
- Internet criminals have widely exploited the Covid-19 outbreaks (phishing and scam campaigns).

DEALING WITH SUSPICIOUS APPS/SOFTWARE

- Downloading malicious apps can compromise your privacy, and that of others, as well as affect your device.
- These apps can steal your data (with your consent).
- The user tends to utilize heavy data usage, which drains the device battery.

NOT OVERSHARING

1. Keep personal information to yourself.
   - Remember that anything you post on the internet is in the public domain, even if you use privacy settings. While social media is a great way to stay in touch with friends and family, other people may also be able to see what you post.

2. Keep your social media profiles private.
   - Keeping your social media profile private means that you will be sharing with only a select few people (your friends or approved followers).

3. Turn off automatic location functions.
   - If you need to use your GPS, just turn the location back on.
   - Consult the user guide in your phone or tablet for more information about how you can turn off location sharing features.

4. Do not check in everywhere you go.
   - Think carefully about where you check in. Limit check-ins to special events and trips.
   - Additionally, do not check in from places far from home, since this will alert potential criminals that you will not be returning to your home any time soon.

5. Do not share pictures of others without their consent.
   - Posting of pictures may compromise the security of others.
   - Some photos may violate children's rights etc.

6. Do not share information of others without their consent.
   - Posting of others' IDs or any other material or information may constitute a crime.

7. Do not post anything related to your clients/students or your work.
   - Value the privacy of your clients/students, as well as your functions.
   - Respect the privacy and integrity of your organization.

8. Consider who is going to see your posts.
   - If you want to share personal matters or those relating to your work, do so in private messages (but not in group chats).
   - Avoid sharing posts on social media that may be inappropriate for your "friends list" or those which are too personal.

PROPER DISPOSAL OF FILES

1. Deleted files on storage devices may be recovered. Five file recovery free programs:
   - Recuva
   - Test Disk
   - Pandora File Recovery
   - R-Linux
   - Glary Undelete

Note: Do not forget to empty your recycle bins.

2. Confidential documents should be shredded (if possible).
    - Paper containing confidential documents must not be recycled.

IMPOSING RESTRICTIONS

- Do not allow unauthorized persons to get inside your work area because confidential documents may be all around your work area.
- Do not allow unauthorized use of your computer or work area or table.
- Lock computers when you are away.

A SECURE AND EFFECTIVE FILING SYSTEM

A good filing system is not only organized but also secured.

- Secure physical documents in proper receptacles.
- For soft copies, password protection is recommended, as well as backups.
- Organize "folders."

OFF THE GRID STORAGE

- Restricted data is best stored in an offline computer. Malwares can steal data from your computer and compromise your operation and your client's privacy. If this cannot be avoided, the user must take extra care in internet browsing.

RESTRICTED VIEW

- Computer monitors must not be in the direct view of clients; otherwise, this may expose data to those in line or to other clients if you fail to close or minimize the window.

CLEAN DESK POLICY (CDP)

- Clear your working space before you leave.
- Put on tabletops only documents that you actually need.

PORTABLE STORAGE DEVICES

- Use portable storage devices responsibly.
- Do not store highly sensitive information on portable storage devices for use outside of the office, if possible.
- Dispose storage devices properly when no longer needed.

Reference:

Atty. Edgar Pascua II
Private Matters: Data Privacy in an Online World
CEAP Webinar Series, August 4, 2020

ALUMNA IN THE NEWS

Teresa Ignacio-Gonzalvo (HS 1969, BSN 1974) was elected the President Elect for the Philippine Nurses Association of Virginia, as well as Chair of the Constitution and By Laws Committee. Concurrently, on a national level, she was appointed the chair of the Ethics Committee of the Philippine Nurses Association of America.

Techie says, "Proud to serve, paying it forward to our *kababayans*. Thanks to our great Paulinian Nursing education!"

Techie (standing extreme right)
with the Philippine Nurses Association of Virginia's Circle of Presidents.

SHARING…SHARING…SHARING

From the Philippine Oncology Nurses Association

Dr. Marichen Dychangco shares the following invitation:

The Philippine Oncology Nurses Association, in collaboration with ICU Medical, presents to you a PONA Update entitled: "Closing the Loop in Cancer Care: Enhancing Competencies in Chemo Infusion." This will be held via zoom on October 30 and 31, 2020 from 10:00 am to 12:00 nn. Due to the nature of the activities of the program, we will only be accepting a limited number of participants on the platform.

Please register using the link: https://forms.gle/FYZdLkvSz7WBchfKA

The Philippine Oncology Nurses Association, Inc. (PONA) is a non-stock, non-profit organization composed of nurses involved in/or interested in the care of cancer patients and their families. It is a duly-recognized specialty organization of the Philippine Nurses Association (PNA) and a member of the Asian Oncology Nursing Society (AONS).