



## CYBERSECURITY TRAINING FOR TEACHERS (CTT)

---

### SECURING ONLINE COMMUNICATION AND PII

#### Objectives

At the end of this module, the learner should be able to:

- Secure their online communication.
- Protect their personal and organizational information.
- Implement measures to secure their PII.

The world has been a global village because of the easy, quick and friction-less communication we are able to have with each other regardless of how far we are. We are constantly in communication with each other. Think of the email you sent your students regarding an assignment, of the pictures you were able to share with your loved ones over WhatsApp, of the online class you taught on Zoom, of the picture you just liked on Facebook or of the call you just made. All of this is communication over existing channels.

While all of this is amazing, how do we make sure that the communication we have over the internet is safe and secure?

These are some ways to have secure online communication:

1. **Be cognizant of the information you are sharing.** Given the nature of our society, we need to be critical of what we tell people, friendly or hostile, about ourselves. Limit with who you share very personal information and even then, make sure it is with people you trust.
2. **Cultivate good password habits.** Employ the use of password managers and use strong, unique, complex and frequently rotated passwords. Use two-factor authentication or biometric authentication whenever possible. When it comes to sharing passwords especially with your co-workers or your students, do so in a safe and secure channel that is private to involved parties. Password managers can also be utilised for sharing passwords securely.



## CYBERSECURITY TRAINING FOR TEACHERS (CTT)

---

3. **Trust your instincts.** If something doesn't feel right, it probably isn't. If an email appears sketchy, examine it further. If someone you are talking to has shady tendencies, maybe they are sketchy. If a software you just installed is making your system react oddly, examine it further. Trust your instinct.
4. **Separate your email accounts according to purpose.** Have a personal email address and a work address. Some people go further and have email addresses for financial purposes and an email just for signing up for apps/services you want to try but aren't too sure or those which might spam you. This makes it easier to quickly recognize phishing emails. If a phishing email claiming to be from your bank gets into your work email, you immediately know it's fake.
5. **Learn to identify click bait and how to not fall prey.** Click-bait comes in all sorts of ways, not just catchy headlines. They can be in emails, on Facebook and even on messaging apps aiming to trick you into clicking links. Don't click links in emails or text messages, unless they come from a source you're sure of. Even then, always be cautious; your trusted source might have been compromised, or the message might be a fake.
6. When sharing files with your students or co-workers, **make sure you use secure file-sharing methods.** Cloud services such as DropBox and Google Drive are good for daily use and have security features embedded. Additionally, you can put in place access control methods that define who has what rights to your files and folders e.g only the class representative can add or delete files as required while the rest of the class can only view the contents. Always double-check permission setting on important files and run audits to see who has been accessing your files. If a file is no longer needed, delete it completely.
7. **Use communication applications and software that have end to end encryption enabled.** End to end encryption is a secure method of communication that prevents third parties from accessing data while it's being transferred from one end device to another. Messaging apps such as WhatsApp and Signal as well as email services such as Tutanota ensure end to end encryption of messages which reinforces security when communicating.



## CYBERSECURITY TRAINING FOR TEACHERS (CTT)

---

### SOCIAL MEDIA AND PRIVACY

Social media is a great tool for educators. It can be used as MAny are on social media for personal and professional use and for the most part, it is great. Professionally, social media can enhance your network, engage you in important discussions, extend your own learning and even provide a platform for class projects. As educators, how do we ensure that in our social media use for both professional and personal use, we still maintain appropriate use and maintain security? Social media services and apps can also be used as educational tools.

#### 1. Appropriate use.

Educators have responsibilities that can cause them to think twice about social media. It is important to put into consideration the following:

- What is appropriate to post?
- With whom should you share content?
- Who should you interact with?
- How do you control who has access to what you post?
- Should you follow/interact with your students at all?
- What about parents and colleagues?
- Are there posts you should avoid posting/reposting or sharing?

#### 2. Protecting your privacy on social media.

The first thing before using any social media service is to understand its privacy settings. Almost all services have some control over who can see what you post. When posting, there are limits on who sees what you post but if you are worried about the nature of your post, it is best to avoid it completely.

#### 3. Interacting with students, parents and colleagues

Regardless of the policies in place regarding interaction with students, it is always important to think about the post you are sending before sending them. Some teachers use social media to discuss classroom projects, class updates and share resources with students. In this scenario, it would be



## CYBERSECURITY TRAINING FOR TEACHERS (CTT)

---

advisable to set up Pages or Groups that their students can join without having to ‘friend’ their students. When it comes to parents and colleagues, it is paramount to maintain professionalism and always be aware of your audience and only post what is appropriate.

### 4. Teaching your students about Internet safety

Students also need to understand the importance of critical thinking while using social media. While it is very enjoyable for them and they tend to share a lot of personal information on social media, it is important as educators to inform them of the potential dangers lurking on these sites. Additionally, emphasizing kindness, critical thinking and personal responsibility when using social media and the internet in general is all it takes.

## PERSONALLY IDENTIFIABLE INFORMATION (PII)

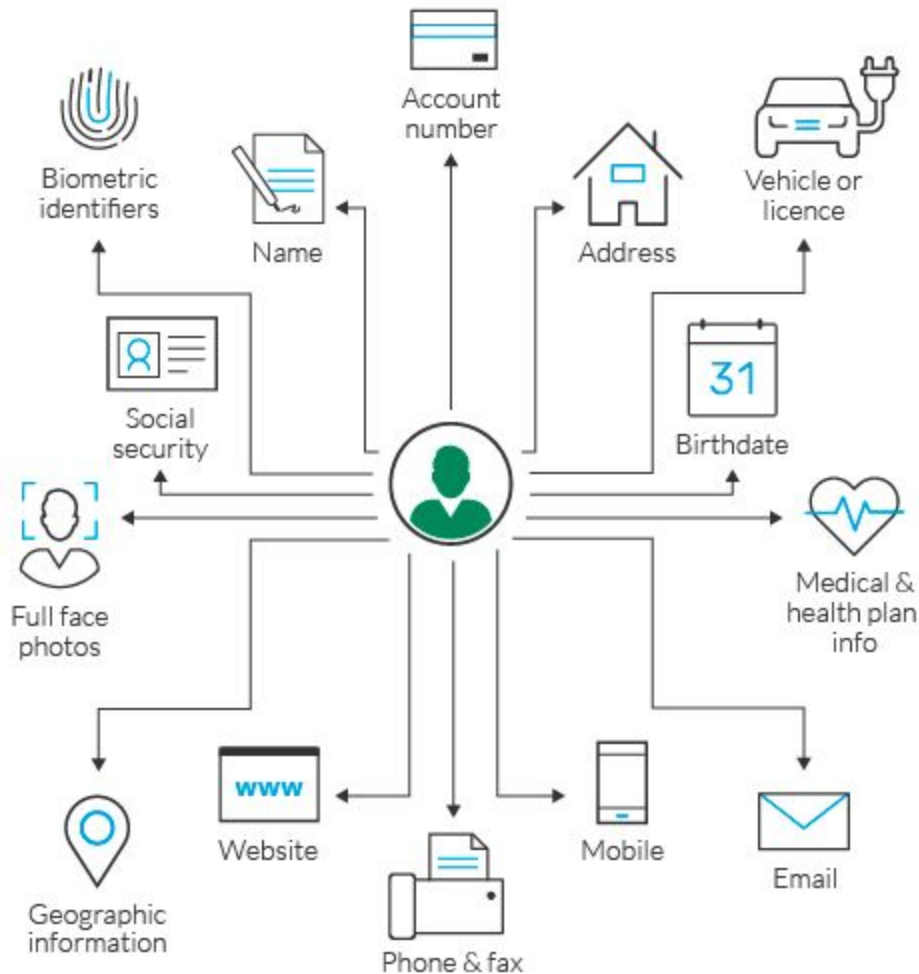
We should be very critical about the information we share with others regarding ourselves. Information that identifies you uniquely is called **Personally Identifiable Information**. This includes your name, physical home address, email address, telephone numbers, date of birth, marital status, and other information relating to your medical status, family members, employment, and education. This data can be used on its own or with other information to identify, contact or locate you in context. For example, your physical home address paired with your work address, can aid in identifying when you are home and when you may be at work.

According to the [NIST PII Guide](#), the following items definitely qualify as PII, because they can unequivocally identify a human being: full name (if not common), face, home address, email, ID number, passport number, vehicle plate number, driver’s license, fingerprints or handwriting, credit card number, digital identity, date of birth, birthplace, genetic information, phone number, login name or screen name.



## CYBERSECURITY TRAINING FOR TEACHERS (CTT)

---



### *What Is Considered PII?*

PII (Personally Identifiable Information) can either be sensitive or non-sensitive. Sensitive PII identifies you uniquely and directly such as your ID number, employment number, a student's ID number, driving license, passport number and even your medical records. Non-sensitive information is easily accessible from public sources such as the internet and is not as delicate as sensitive PII. Non-sensitive information includes your gender, race, date of birth e.t.c. Non-sensitive PII is not enough to identify an individual but combined with sensitive PII, it makes it very easy.



## CYBERSECURITY TRAINING FOR TEACHERS (CTT)

---

### Potential dangers of exposure of PII

PII is very critical and marketable these days. When this data is stolen either in phishing schemes or data breaches, it can provide attackers with enough information to perform identity theft which may enable them to take out huge loans in your name, file fraudulent insurance claims or perform other serious crimes. Additionally, with the amount of information that one can post about themselves online, it is easy to become a victim of stalking without even being aware of the risk.

### Securing and Safeguarding PII

1. Before you send that social media post, think first. Assess the image or the information you want to share and consider whether it is safe and 'vague' with regard to PII before sharing it especially on social media. Additionally, don't fill your social media with too much information about yourself.
2. Shred all files that have PII before discarding them. Physical documents such as bills, receipts, physical copies of your personal documents, bank statements e.t.c can be stolen if an individual's home is broken into. Cybercriminals will literally dump the businesses' trash in search of sensitive data because of how profitable PII is.
3. If you have access to others' PII, such as that of your students, ensure you protect and secure it using good data backup procedures, by safely destroying old media with sensitive data, employing appropriate and thorough device security measures and having accountability measures in case of mishandling of data.
4. Educate your students on the importance of online privacy. Preteens and early-teenagers are most susceptible to oversharing especially on social media. It is important that they understand how to protect themselves online, and the detrimental consequences that could come from sharing too much personal information online.
5. Read through the privacy statements of the applications you use. It may look tedious but we tend to agree to Terms of Use without truly understanding what we are consenting to.
6. When using a shared or public computer, do not click "Remember/Save Password" as this saves your credentials on the browser.



## CYBERSECURITY TRAINING FOR TEACHERS (CTT)

---

7. Always completely sign out after each session when accessing the internet on a shared or public computer.
8. Don't use the same password for more than one system even though the login ID is the same. For example if students use their studentID student111@schoolABC.org to login to their moodle session and use the same ID for login to Zoom for an online learning session, the password for Moodle and Zoom must be different.

### Discussion Question:

1. What other examples can you give of sensitive and non-sensitive PII? In what ways do you think people share PII over social media without being aware?
2. How can you help your students understand the risks of oversharing personal information especially on social media?