



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Roles of Students, Teachers, Parents and Guardians

Key Role Players

Parents, teachers and guardians are responsible for whatever activities students take part in on the internet while learning online. They should ensure safety of students online. Students too have a role to play so that they don't put themselves or others in danger while learning online.

We will begin by looking at the role of teachers. Teachers should introduce and educate students on online safety. This means that teachers should be aware of the risks students may face online and educate them on measures they should take to ensure their safety. Teachers can show students step by step walk-through of different ways they can protect themselves, and provide resources highlighting importance of online safety. This can be through games, animation videos or classroom activities.

Teachers should get parents and guardians involved about the safety of students learning online. They must inform them of any queer behavior a student may show, highlight to them the risks students face online especially without being monitored as a means of creating awareness and direct them to resources available on online children safety.

Roles of Teachers

Technology keeps on evolving at a very fast pace, hence new trends are emerging. What role can a teacher take to ensure students online are protected?

Teachers should educate students on existing online risks and encourage them to be open and honest when they experience any disturbing incidents while online. They should also teach them how to secure themselves while learning online. For example, by using web camera covers to prevent strangers from spying on them. This can be included in the curricula.

Teachers should research and be informed on current trends of online child risks. They should be aware of organizations in charge of children online protection in the



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

region or country and channels they can report an incident a student has faced for example cyber bullying. They should be aware of organizations in charge of children online protection in the region or country and channels they can use to report an incident a student has faced, for example, cyber bullying.

Teachers should get parents involved in the safety of students. They should inform parents of dangers students can face online especially without being monitored and direct them to resources readily available with information on online children safety.

Teachers can provide parents with an online learning guide or plan to help them understand how online learning will occur and encourage them to have an input. This plan can include the different roles and responsibilities of students, teachers, parents and guardians, attendance guidelines, learning expectations, content and timing, assessment and progress monitoring.

Just like the physical classroom, teachers should set rules for a virtual classroom such as no disabling web camera during class sessions. Students ought to be reminded that breaking of rules will result in punishment. An example could be no taking pictures of classmates during an online class session.

Measures an institution can take

1. Secure devices

Teachers should ensure that their devices are secured with strong passwords and are locked when not in use. They can also use software such as antivirus and firewalls to detect software that could harm their devices.

2. Filtering and monitoring

The school internet should be monitored and filtered to ensure students cannot access harmful or age restricted content like drug abuse, hate speech, race discrimination or pornography. Downloaded content and links accessed by the students can be tracked and blocked.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

3. School Policy

The school should have an ICT policy that protects the use of technology in the institution. The policy should guide teachers on use of school devices and student images for education purpose only. The policy can also cover online risks such as bullying, harassment and stalking.

Teachers should monitor students while online and examine the behaviours they exhibit. They should also be up to date with risks minors face online in order to understand when a student shows any kind of foreign behaviour.

4. Online personality

Teachers should be aware that anything they post on the internet could affect their reputation and that of their school. They should therefore separate their personal life from their work life and be professional at work.

5. Training

The school can train all staff on online safety and internet risks often. The school can appoint an online safety coordinator to conduct these trainings to students, parents and school staff. This should include how to report cyber incidents and channels to use.

6. Audit the school systems

The institution should conduct regularly audit of the school systems to ensure there is no loop holes an attacker may use to hack such as non-updated computers.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Ways to improve teacher-parent communication

Teachers should include parents on the progress of young learners. There are different methods that can be used to ensure effective communication between educators and carers. These are:

1. Social media platforms

The school can post updates, news, student information and key events on their social media like Twitter or Facebook page

2. Parent portal

The school can develop an application that enables a carer to be updated with their student's progress in school such as extra curricula activities, grades, attendance and assignments. The parents can communicate with the teachers on their child's progress in school.

3. Mobile application

A mobile application is an effective method for teachers to communicate with busy parents. This will enable them to have knowledge on the student's performance and get instant feedback from the teachers.

4. School Management System

This is functional method for parents-teachers communication. A parent can track student's performance on each subject and learn on teachers taking the subjects. The system can generate a graphical view of the student's progress at the end of every semester, term and academic year.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Roles of Parents and Guardians

Parents ought to learn and understand the risks their children may face while learning online. One way is to familiarize with cases that have occurred, and the effects or harm caused. They should talk and teach students regularly about dangers they are likely to face and the harm it can cause. Students should be encouraged to be open and inform their guardians or parents of any disturbing experiences they come across online.

Parents should set reasonable rules and guidelines for computer use by their children. This can be time to access the internet and digital devices. This will ensure they don't spend too much time on the internet and curb internet addiction which may lead to mental instability. Parents should familiarize with student friendly websites that can be used for learning and entertainment. These websites filter content thus preventing access to inappropriate materials by the students.

Parents and guardians should install parental control software that monitors what students do and prevent them from accessing harmful websites. They should also learn and familiarize with online platforms the students use and monitor their activities by looking through history to see the sites they have visited. Examples of parent control software are: Qustodio, Open DNS Family Shield, KidLogger, Spyrix Free Keylogger and Kaspersky Safe Kids. These softwares are available in free and paid version whereby the free version has limited features.

Parents and guardians should be open to their children. They should be able to communicate freely and honestly about online risks and incidents that have occurred. Parents are responsible for introducing children to online safety and inform them of the do's and the don'ts while learning online. For example, children should not give information about who they are or where they live to strangers online. They should rather report such incident to their parent or guardian.

Parents should take interest in their children's online activities and the platforms they use e.g. social media platforms. This will help them understand the kind of risks they are exposed to. Parents should ensure the children are not accessing age



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

restricted content or websites. They should inform the children on children friendly search engines like kiddle that monitors and filters content to be children friendly.

Parents should learn to do the following in social media platforms:

1. Report inappropriate and offensive posts
2. Block a user
3. Keep information and accounts private

Parents should go for cyber and online safety awareness training offered by ministry of ICT or relevant institutions to learn of emerging online risks and challenges for children and measures to take to ensure online child protection.

A parent should ensure the following once he or she has purchased a new device for the student:

1. Set rules device usage
2. Ensure password protection has been set up
3. Update the device to the latest software version
4. No downloads of apps without approval from carers
5. Turn off location services, Wi-Fi and blue-tooth when not in use

There are different organizations responsible for child online protection and platforms that can be used to report cyber incidents. Parents should learn about such platforms and organizations in the country or region. Lastly, they should set reasonable rules and guidelines for computer use by students such as the time to access the internet and devices.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Roles of Students

Students also have a role to play in ensuring they don't jeopardize their safety while studying online. They should report any uncomfortable experience online to their parents, teachers or guardians.

Rules are always put in place to ensure safety of the students. Therefore, students must adhere to rules set by parents, teachers or guardians on internet use or online classroom sessions.

Students should not give personal information such as address, phone numbers or emails to strangers online and refrain from posting and sending pictures and videos of themselves to strangers on the internet.

Students should not open an email from someone they do not know. This is because it could contain an attachment with malicious code or a pathway for a cyber predator to communicate with young learners.

Students should never agree to meet with someone they have met online. This could put their lives in danger in the hands of a cyber predator.

We all should be careful on how we use the internet as the internet never forgets!