



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Laws on child online protection

As technology keeps on progressing, there is a need for blending technology in teaching and learning. One way is by students learning online using smart devices and computers. This has made learning and teaching easier especially during the Covid-19 pandemic. However, as students learn online, there are several risks they may face like cyber bullying, violent content, child pornography and cyber-attacks.

Laws are used to rule and govern how a country or state will run by protecting people and maintaining public order. Countries and states around the world have implemented laws that ensure the protection of children while online. Most of these laws are acts and we will look at different acts in countries within the different commonwealth regions including Africa, Asia, Europe, Pacific, Caribbean and Americas.

Non-Governmental organizations have also highly contributed to ensuring child online protection. For example, the International Telecommunication Union (ITU) - a United Nations agency that came up with guidelines for parents and educators on Child Online Protection. The key objective of the guidelines is to identify risks and vulnerabilities to children in cyberspace, create awareness, develop practical tools to help minimize risks and lastly share knowledge and experience.

These guidelines are for children, parents, guardians and educators, industry and policymakers and they aim at setting up a base for safer and secure internet services and technology for children.

The official guidelines for parents and educators documentation can be found on this [link](#).

The organization has also developed a [workbook for students](#) (9-12years) to teach them about their rights and safety online by providing six scenarios which they may face while learning online. The scenarios are:

- Right to play online
- Managing screen time
- Exposure to inappropriate content
- Right to use digital media to learn
- Privacy
- Adult role modelling of positive use of digital media

There is also a [teacher's guide](#) that provides online safety exercises in a classroom setting with the aim of inspiring students to tackle online safety through their teachers.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Most countries in the commonwealth have collaborated with ITU with the aim of developing localized guidelines for child online protection.

Commonwealth Regions

1. Africa

For this region, we will look at laws and measures taken by Kenya to ensure child online protection.

In Kenya, the Communication Authority of Kenya, an ICT regulator under the Ministry of ICT, is responsible for ensuring child online protection. One way the authority does this is by creating awareness through campaigns on risks that children are exposed to while accessing online services like virtual learning.

The authority works closely with several local institutions like mobile service providers and the Department of Children Services to create awareness. The authority has a website that a parent, guardian or teacher can use to report any cyber risk a student has faced while learning online.

The screenshot shows the website of The National KE-CIRT/CC, which is the Kenya Information and Communications Act, 1998, mandated by the Communications Authority of Kenya to develop a national cyber security management framework through the establishment of a national Computer Incident Response Team (CIRT). The website features a blue header with the organization's name and a tree icon made of social media icons. Below the header is a navigation bar with links: Home, About Us, Library, Alerts & Advisories, Publications & Guides, and Contact Us. The main content area is titled 'Report An Incident' and includes a form with fields for Name (required), Organization (required), Contact Number (required), Email (required), Subject, Category, and Remarks. There are also buttons for 'Report An Incident', 'Report A Vulnerability', and 'Sign Up To Receive Regular Updates'. A sidebar on the right contains a 'Help' button and a 'Subscribe To Newsletters' button.

[Image from ca.go.ke]

The Children's Act No.8 of 2000 makes provision for parental responsibility, fostering, adoption, custody, maintenance, guardianship, care and protection of children. This provision extends to protecting children while learning online.

The Data Protection Act No. 24 of 2019 says the following when it comes to protection of children's data.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

No. 24	Data Protection	2019
33. (1) Every data controller or data processor shall not process personal data relating to a child unless — (a) consent is given by the child's parent or guardian; and (b) the processing is in such a manner that protects and advances the rights and best interests of the child. (2) A data controller or data processor shall incorporate appropriate mechanisms for age verification and consent in order to process personal data of a child. (3) Mechanisms contemplated under sub-section (2) shall be determined on the basis of— (a) available technology; (b) volume of personal data processed; (c) proportion of such personal data likely to be that of a child; (d) possibility of harm to a child arising out of processing of personal data; and (e) such other factors as may be specified by the Data Commissioner. (4) A data controller or data processor that exclusively provides counselling or child protection services to a child may not be required to obtain parental consent as set out under sub-section (1).		

Processing of
personal data
relating to a child.

[Image from kenyalaw.org]

2. Asia

For this region, we will look at laws and measures present in India to ensure child online protection.

In India, the Information Technology Act 2000 Section 67 B talks about punishment for anyone who facilitates abuse of children online. He or she may be imprisoned for up to seven years and fined up to ten lakh rupees (\$13539.00).



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.—Whoever,—

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

25

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

[Image from indiacode.nic.in]

The National Policy of ICT in Schools (2012), focuses on regulating ICT to protect students from online risks. It has provisions for regulating and monitoring access to the internet.

The National Cyber Security Policy (2013), covers on the prevention, investigation, and prosecution of cybercrimes. This includes cyber-crimes against children and online students. The law enforcing agencies e.g. the police, will investigate these crimes and collate information for prosecution.

The Computer Emergency Response Team (CERT) website can be used to report cyber incidents faced by students while learning online. CERT in India conducts training to create cyber security awareness. Such training impacts teachers and parents on cyber security and ways they can protect their children online.

3. Europe

For this region, we will look at laws and measures present in the United Kingdom to ensure child online protection.

In the UK, Child Exploitation and Online Protection Command (CEOP), a command of National Crime Agency, is responsible for taking national and international online child sex offenders to court. This includes persons involved in production, watching, sharing and distribution of such material. Anyone, be it a child, parent or guardian can report child online exploitation concerns like inappropriate or potentially illegal activity with or towards a child online to the CEOP safety centre.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

Sexual Offences Act 2003, Protection of Children Act 1978, Criminal Justice and Immigration Act 2008, and Malicious Communications Act 1988, can be used in the court of law to support cyber related crimes against a child.

Cyber related concerns related to a student can reported on the Computer Emergency Response Team website.

4. Pacific

For this region, we will look at laws and measures present in New Zealand to ensure child online protection.

In New Zealand, the Crimes Act 1961 (Section 124B) focuses on indecent communication with young people under 16 years in whatever manner (this includes through online means). This law is used to protect students against online predators who are after gullible students. It is therefore important to create cyber awareness in schools and homes to protect students from such incidents.

The Films, Videos, and Publications Classification Act 1993 (Section 127) protects children online by posing a hefty punishment of a fine of up to \$30,000 for exhibiting an objectionable publication to a minor. A different section of the same act considers publication as age restricted if it has highly offensive language that may cause harm to persons under a certain age. This act can be used to protect students online from sensitive adverts and videos.

The New Zealand Cyber Security Strategy aims at ensuring protection of children online through the Online Child Exploitation Across New Zealand (OCEANZ). This is a specialized police unit responsible for protecting children from online abuse.

How then can a teacher, guardian or parent report a cyber incident? CERT NZ provides a website where one can report cyber incidents. Another way is through filling forms available on the National Cyber Security Centre website and sending them through [email](#) indicated on the forms.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)



CYBER SECURITY INCIDENT - REPORT FORM

This form can be used to report cyber security incidents to the National Cyber Security Centre (NCSC), which is part of the Government Communications Security Bureau.

If you would like to request assistance from NCSC in relation to the incident, please use the Cyber Security Incident - Request for Assistance Form (Evaluation Services). You do not need to complete this form if you complete a Request for Assistance Form.

Send this completed Cyber Security Incident Report form to NCSC by email (Incidents@ncsc.govt.nz), or post (National Cyber Security Centre, PO Box 12-209, Wellington 6144). If the completed form contains confidential or classified information please contact NCSC to arrange an alternative method of receipt.

If you have any questions about this Cyber Security Incident Report Form, you can contact NCSC by phone on (04) 498 7654.

PART 1: YOUR CONTACT DETAILS	
YOUR ORGANISATION	
Organisation Name:	Click here to enter text.
Physical Address:	Click here to enter text.
Postal Address:	Click here to enter text.
CONTACT PERSON	
First Name:	Click here to enter text.
Last Name:	Click here to enter text.
Job Title:	Click here to enter text.

[Image from ncsc.govt.nz]

5. Caribbean & Americas

For this region we will look at laws and measures present in Canada to ensure child online protection.

In Canada, the Criminal code 1985 touches on PII in regard to credit card and passwords, unauthorized use of computer and identity theft. This code can be used in a court of law to prosecute anyone who risks the safety of a student while studying online.

Canadian Centre for Cyber Security oversees the handling of cyber incidents. Reported incidents are also analysed before forwarded to responsible law enforcement agencies. This includes risks students can face online such as identity theft or fraud.

Online concerns touching on online sexual exploitation of students or children can be reported using the cybertip website. This platform is operated by the Canadian Centre for Child Protection. Reports made through cybertip are analysed based on the criminal code to determine if the incident is illegal. If it is, it is forwarded to the law enforcement agency.



CYBERSECURITY TRAINING FOR TEACHERS (CTT)

cybertip!ca® CANADA'S NATIONAL TIPLINE FOR REPORTING THE ONLINE SEXUAL EXPLOITATION OF CHILDREN

DONATE EN FRANÇAIS

CLICK HERE TO REPORT

ABOUT US CHILD SEXUAL ABUSE INTERNET SAFETY PROJECTS PARTNERS REPORTING

Welcome to Cybertip.ca

Canada's tipline to report the online sexual exploitation of children.

Supported By: BellMTS

Search

Sign up to receive Cybertip.ca ALERTS

Do you provide an Internet Service? REPORT HERE

Concerned about a sexual (or nude) picture being shared online?

Talk to your teens about the harm of sharing others' nudes.

CLICK TO LEARN MORE

Forward image to group? YES NO

[Image from [cybertip.ca](https://www.cybertip.ca)]

Case Study on Child Online Abuse

1. [Cyber Bullying](#)
2. [Cyber predator](#)

Additional Reading Material

1. [Child Online Protection Act - USA](#)
2. [Data Protection Act - Kenya](#)
3. [Information Technology Act - India](#)
4. [Criminal code - Canada](#)
5. [Crimes Act - New Zealand](#)
6. [Films, Videos, and Publications Classification Act - New Zealand](#)
7. [Protection of Children Act - United Kingdom](#)
8. [Guidelines for parents and educators on Child Online Protection by ITU](#)