Be Safe in Cyber World

Do's and Don'ts for Teachers

Central Institute of Educational Technology, NCERT
Sri Aurobindo Marg, New Delhi - 110016

DEVELOPMENT COMMITTEE

Chairperson

Prof. Amarendra Behera, Joint Director, Central Institute of Educational Technology, NCERT, New Delhi.

Member Coordinator

Dr. Angel Rathnabai, Assistant Professor, Central Institute of Educational Technology, NCERT, New Delhi.

Member

Dr. Indu Kumar, Associate Professor and Head, Department of ICT& Training Division, Central Institute of Educational Technology, NCERT, New Delhi.

Dr. Mohd. Mamur Ali, Assistant Professor, Central Institute of Educational Technology, NCERT, New Delhi.

Dr. Rejaul Karim Barbhuiya, Assistant Professor, Department of Education in Science and Mathematics, NCERT, New Delhi.

Dr. Ramanujam Meganathan, Associate Professor, Department of Education in Languages, NCERT, New Delhi.

D. Varada M. Nikalje, Associate Professor, Department of Elementary Education, NCERT, New Delhi.

Ms. Surbhi, Assistant Professor, Central Institute of Educational Technology, NCERT, New Delhi.

Mr. I L Narasimha Rao, Project Manager II, Center for Development of Advanced Computing (CDAC), Hyderabad.

Ms. Sujata Mukherjee, Global Research and APAC Outreach Lead, Google India Pvt Ltd, Hyderabad.

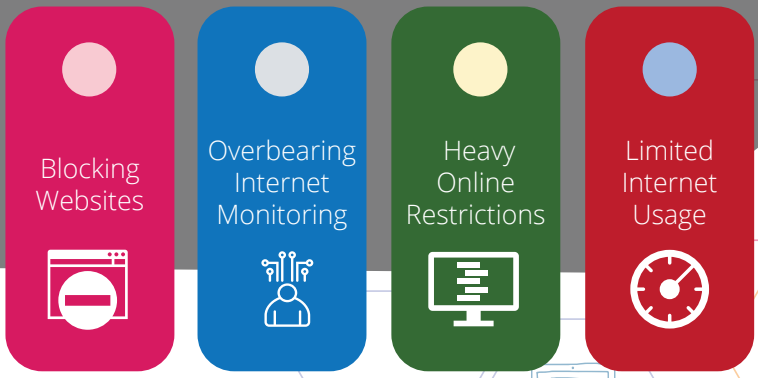
Capt. Vineet Kumar, Founder and President, Cyber Peace Foundation, Ranchi, Jharkand.

Ms. Chandni Agarwal, National ICT Awardee and Head, Department of Computer Science, Maharaja Agrasen Model School, ,Delhi.

Ms. Vineeta Garg, Head, Department of Computer Science, Shaheed Rajpal DAV Public School, Delhi.

Be Safe in Cyber World

Technology has broken the barriers of space and nationality to bring us together in ways that were unthinkable 20 years ago. Many of our civilization's greatest advancements in recent years have come from technological breakthroughs. However, there is a flipside to everything. The world of technology can also be dangerous, especially for students. A few slip ups can place a child in real danger. 'Online Safety' is proposed for students who use the internet. Online safety is not just...



Too often educators use these instructions to keep their students "safe." But Online safety is much more than that.

Someone rightly said, "Give a man a fish and you feed him for a day. Teach a man to fish and you feed him for a lifetime."

Similarly, students should be taught to be safe online and to practice good habits while surfing the internet rather than blocking and restricting.

1

Technical Aspects

Do's and Don'ts

1. Use safe search options while searching information on the Internet; also check facts before sharing or forwarding.
2. While performing online banking, shopping or making online payment, check if the website's URL begins with 'https' (the "s" stands for "secure"), also, look for a green address bar or a security certificate (presented by an icon such as an unopened lock) in the browser window that ensures secure connection. Double click the certificate to make sure the name on the web address matches the certificate.
3. Do not use same password for different online transactions.
4. Use a strong and unique password combinations of numbers, uppercase, lowercase letters and special characters for each account.
5. Use separate email accounts for personal and official purpose. Never use your official email address for social media sites.
6. Avoid using free, unsecured Wi-Fi for shopping or banking on the Internet and also for logging into your social media profiles.

1

Technical Aspects

7. Delete old accounts that you do not use any more.
8. Obtain software from trusted sources. Always scan files before opening them.
9. Access your bank's website by manually typing its URL in the address bar. Never access it from an email or a text message.
10. Never click on links or download attachments in unwanted, unexpected emails, even if such emails appear like they are from a known source.
11. Take regular backups of all important files onto offline/ cloud storage.
12. Don't click on 'Keep me logged in' or 'Remember me' options on websites and logout of all accounts..
13. Never use any personal information such as name, date of birth, address, etc., as your password.
14. Never share your personal/bank details on phone, email or SMS, even if the caller/sender seems genuine.
15. Think before you click; stay away from pop-up contests and shady surveys; read the fine print, and close all such pop-ups from the task manager
16. Don't visit inappropriate websites, or websites that you are not fully aware of, just out of sheer curiosity.
17. Don't save your credit/debit card information on websites and web browsers.

1

Technical Aspects

18. Connect to proper wi-fi network, otherwise known as SSID.
19. Have dual or multifactor authentication.
20. Don't use username and password when other options as such as a token, smartcard, PIN, or even user-selected security images are available.
21. Maintain a list of passwords in a safe place, and change them at least quarterly.
22. Ensure that the computer has the latest patches and keep the browser, operating system and antivirus updated.
23. Don't assume that the virus detection software works perpetually with computers.
24. Don't share/upload confidential data in cloud storage systems .
25. Keep a record of all online transactions made and check your bank account regularly.
26. Add a Domain Name System (DNS) service to protect other devices

1

Technical Aspects

27. Lock your screen when you have finished using your computer/ tablet/ phone, and further, set it to lock automatically when it goes to sleep.

28. Don't assume someone else has the responsibility to maintain and protect your data.

29. Do check e-mails carefully to ensure that the source header is from a valid address.

30. Don't fall prey to clicking a link to malicious Web sites that load malware into your computer.

31. Always delete spam emails immediately and empty the trash box to prevent accidental clicking on the same link

32. While interacting with others on discussion forums/ chat rooms, make sure the Caps Lock key is off as typing in capital letters during interaction is considered to be rude.

33. Monitor device usage by students; control time spent on devices.

34. Create restricted or child-only profiles - use options available on browsers, Search, video sites, etc.

35. Ensure that students access only the content/ sites allowed to them

36. Regularly review browsing history on the devices being used by children

2

Ethical Aspects

Do's and Don'ts

1. Don't intentionally use the computers to retrieve or modify the information of others, which may include password information, files, etc.
2. Don't plagiarize i.e., copying information (book, music, video, software etc) from the Internet as it is dishonest and could also be illegal. You could be violating copyright laws.
3. Obtain permission from the original creator if you do want to use the material. Always provide credit and attribution to the original owner of the resource.
4. Never give a fake identity while interacting with people online.
5. Do not make profit from the original work of others
6. Use of material upto 10% may be done by citing the resource. Paraphrase wherever possible.

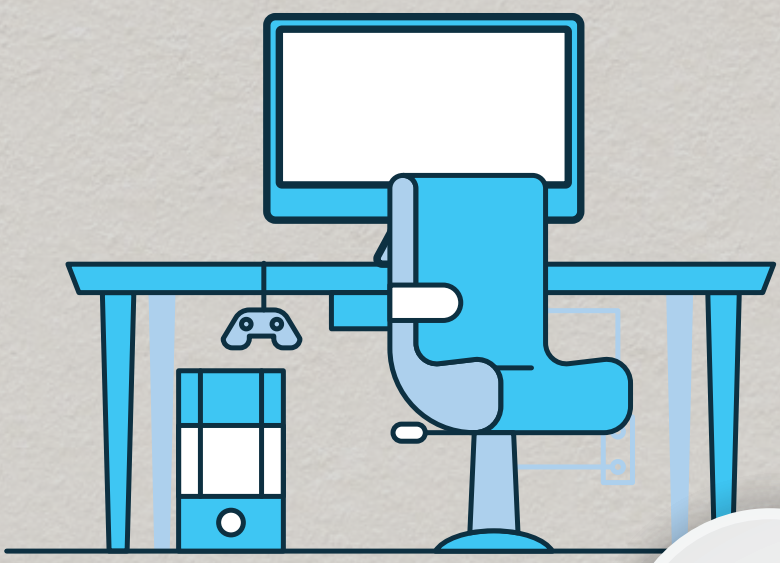
1. Avoid sharing your personal information on social media sites and the Internet in general.
2. Don't cyber bully by being rude,or by using abusive, threatening, humiliating language.
3. Don't engage or argue with cyberbullies as that might encourage even worse behavior.
4. Use the built-in filters to prevent further harassment through email or instant messaging by cyber bullies.
5. Never meet people alone when they are known only through online.
6. Don’t do anything online which cannot be done in the presence of others.
7. Monitor students’ behavioral changes or attitude differences.

4

Legal Aspects

Do's and Don'ts

1. Do report cyber bullying to the proper authorities. Keep a record of every comment received from a cyberbully for taking further action.
2. Never trust e-mails which offer prize money through lotteries of which you are not a participant. Similarly don't pay for the jobs which you have not sought through official channels.
3. Don't trust a site just because it claims to be secure. It may be a 'Phishing' site.
4. Beware of e-mail spoofing.
5. Beware of fake advertisements promoting online purchases.
6. Don't buy any device from unauthorized persons/ dealers.
7. Never read someone else's e-mails even if you know his/her password.



Legal Aspects

Do's & Don'ts

4

8. Never tamper with the computer source records.
9. Never share or alter the collected data without permission of the individual/ organisation.
10. Never capture, reproduce or transmit the photograph(s) of a person without his/ her consent.
11. Never publish or transmit vulgar material in electronic form.
12. Report any objectionable child-abusive materials in electronic form to the concerned authorities.
13. Don't send any threatening, abusive or defamatory emails.
14. Don't hide/ conceal computer hardware belonging to school.
15. Never infringe on any copyrighted materials.

CYBER LAWS

SECTION	OFFENCE	PENALTY
67A	Publishing images containing sexual acts	Imprisonment up to seven years, or/ and with fine up to Rs. 1,000,000
67B	Publishing child porn or predating children online	Imprisonment up to 5 yrs and with fine up to Rs. 1,000,000 on 1st conviction. Imprisonment up to 7 yrs, or/ and with fine up to Rs. 1,000,000 on 2nd conviction.
67C	Failure to maintain records	Imprisonment up to 3 yrs or/ and with fine up to Rs. 2,00,000
68	Failure/refusal to comply with orders	Imprisonment up to seven years and possible fine.
69	Failure/refusal to decrypt data	Imprisonment up to three years or/ and with fine up to Rs. 100,000
70	Securing access or attempting to secure access to a protected system	Imprisonment up to ten years or/ and with fine.
71	Misrepresentation	Imprisonment up to three years or/ and with fine up to Rs. 100,000

CYBER SECURITY
MAJOR THREATS
PROTECTING
SAFE PRACTICE
means
include
Spam
Piracy
Malware
Hacking
Scam
Phishing
Copyright Violation
Hoax
E-Mail Bombing
Website Defacement
Morphing
Spyware
Virus
Scareware
Ransomware
Worms
Trojans
Adware
obtaining
Sensitive Information
through
Social Engineering
uses
Websites Spoofing
E-mail Spoofing
Click jacking
Tab Napping
Instant Messaging
Phone Call
like
Password
User Name
Credit Card Details
Cyber Crime
Online Predators
Sexual Activities
Grooming
Harassments
Threats
Cyber Bullying
Name Calling
Teasing
Insults
Lies
Rumors
Threats
Repeated Harassment
is
Cyber Stalking
including
False Accusations
Slander
Libel
Defamation
through
Websites
IM
E-mails
Online Groups
Phone
Pornography
Fake Account
Identity Theft
from
committed
for
Money
Curiosity
Revenge
Attention
Fun
Information & Devices
from
Modification
Destruction
Unauthorised Access
Disruption
Disclosure
Use/Misuse
Theft
use
Password
do not
Share
should be
Changed
save
Securely
shoud be
Strong
for
Desktop/ Laptop
use
Firewall
protect
Password
update
Software
backup
Data
no to
Pirated Software
use current/ updated
Operating System
use & update
Antivirus
regular/ automatic
Scan
legal
Cyber Laws
in
Social Media
avoid
Strangers
do not share
Personal Informtion
use
Privacy Options
Security Options
ensure
User to be Old Enough
any
Threats
inform
Parents
approach
Cyber Police
save
Chat Screen
do not
Be Scared
in using
Internet
use
Latest Browser
use
Content Filtering
avoid
Friendship
with
Unknown People Online
avoid
Meeting in Person
secure
WiFi
use
E-mail Tracer
update
Browser Pluggins
never visit
Untrusted Website
check
URL
beware of
Spy Camera
clean
browser's cookies and cache
do not open
E-mail Attachments
from
Unknown Persons
avoid
Referral Links
instead
Type the URL
Mobile Devices
format
Before Discarding
download app from
Authorised Store
access only
Authorised WiFi
use
Auto Lock
do not accept
Call from Weired Number
and do not
Call back
record
IMEI Number
switch on
Bluetooth
only
When Needed
CC:BY:SA-M.U.Paily

www.ictcurriculum.gov.in

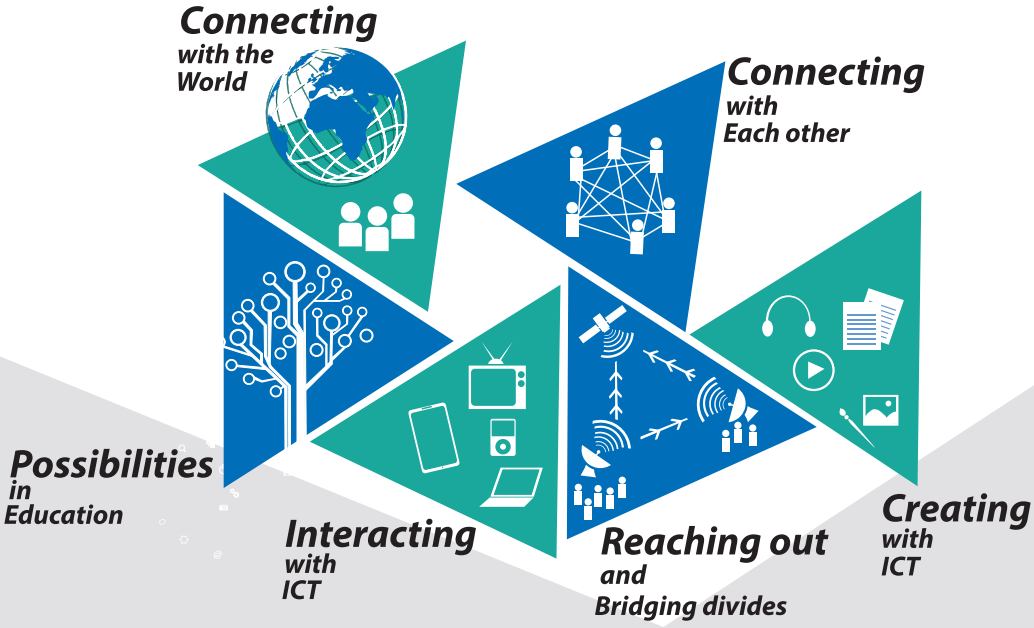
Curricula for Information and Communication Technology (ICT) in Education

सत्यमेव जयते

Department of School Education & Literacy
Ministry of Human Resource Development
Government of India

The model curricula for ICT in Education is a significant vehicle for realization of the goals of the Digital India Programme. The curricula is rolled out for teachers and students to build capabilities in using ICT to enhance teaching –learning and interact critically with information.

The Curricula is organised into six strands:



Central Institute of Educational Technology
National Council of Educational Research and Training
Sri Aurobindo Marg, New Delhi - 110016

For More Details

www.ncert.nic.in
www.ciet.nic.in
www.ictcurriculum.gov.in
www.infosecawareness.in
www.cyberswachhtakendra.gov.in