



# Be Safe in Cyber World

Do's and Don'ts for Teachers

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

# Be Safe in Cyber World





1

# Technical Aspects

1. Use safe search options while searching information on the Internet. Also check facts before sharing or forwarding.
2. While online banking, shopping or 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 letter and special characters for each account(s).
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.
7. Delete old accounts that you do not use any more.
8. Obtain software from trusted sources. Always scan files before opening them.

1



## Technical Aspects

- 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 saving your credit/debit card information on websites and web browsers.
- 18.** Connect to wireless using proper 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.



1

## Technical Aspects

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







## Technical Aspects

- 27.** Lock your screen when you're finished using your computer/ tablet/ phone. 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

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 whenever possible.





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





4

## Do's & Don'ts Legal Aspects



https

1. Do report cyberbullying to the proper authorities. Keep a record of every comment received from a cyberbully for taking further action.
2. Never trust e-mails which offers prize money through lotteries of which you are not a participant. Similarly don't pay for the jobs for which you are not in correspondence 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





## Do's & Don'ts Legal Aspects

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 filthy materials 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/ conceive computer hardware belonging to school
15. Never infringe any copyrighted materials

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

---

For More Details  
[www.cyberswachhtakendra.gov.in](http://www.cyberswachhtakendra.gov.in)  
[www.ciet.nic.in](http://www.ciet.nic.in)

