साइबर जगत में सुरक्षा

सुझाव एवं सावधानियाँ शिक्षकों के लिए

केन्द्रीय शैक्षिक प्रौद्योगिकी संस्थान
राष्ट्रीय शैक्षिक अनुसंधान और प्रशिक्षण परिषद्
श्री अरविंद मार्ग, नई दिल्ली -110016

www.ictcurriculum.gov.in

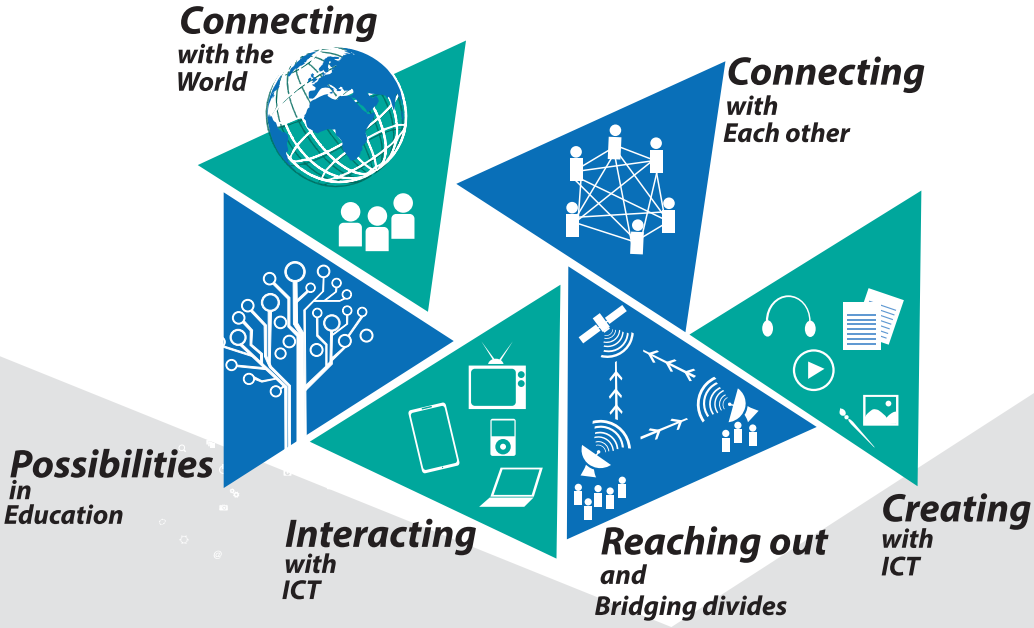
Curricula for Information and Communication Technology (ICT) in Education

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:



विकास समिति

अध्यक्षः

प्रोफेसर अमरेन्द्र प्रसाद बेहेरा, संयुक्त निदेशक, केंद्रीय शैक्षिक प्रौद्योगिकी संस्थान, एनसीईआरटी, नई दिल्ली

सदस्य समन्वयकः

डॉ. एंजेल रत्नाबाई, सहायक प्रोफेसर, केन्द्रीय शैक्षिक प्रौद्योगिकी संस्थान, एनसीईआरटी, नई दिल्ली

सदस्यः

डॉ. इंदु कुमार, प्रोफेसर एवं अध्यक्ष, आईसीटी विभाग, केन्द्रीय शैक्षिक प्रौद्योगिकी संस्थान, एनसीईआरटी, नई दिल्ली

डॉ. रेनाउल करीम बड़बुईया, सहायक प्रोफेसर, केन्द्रीय शैक्षिक प्रौद्योगिकी संस्थान, एनसीई. आरटी, नई दिल्ली

डॉ. आर. सी. शर्मा, प्रोफेसर, डा. बी. आर. अम्बेडकर विश्वविद्यालय, दिल्ली

डॉ. सर्वेश मौर्य, क्षेत्रीय शिक्षा संस्थान (एनसीआरटी), मैसूर, कर्नाटक

डॉ. जितेन्द्र पांडे, सहायक प्रोफेसर (कंप्यूटर विभाग), उत्तराखंड मुक्त विश्वविद्यालय, हल्द्वानी, उत्तराखंड

डॉ. प्रवीण कुमार, सहायक प्रोफेसर (अंग्रेजी व संचार कौशल) महर्षि मारकंडेश्वर विश्वविद्यालय, अम्बाला, हरियाणा

श्री हरि कृष्ण आर्य, निदेशक ज्ञानोदय इंटरनेशनल स्कूल, हनुमानगढ़ टाउन, राजस्थान

सुश्री कुनिका, जूनियर प्रोजेक्ट फेलो, केन्द्रीय शैक्षिक प्रौद्योगिकी संस्थान, एनसीईआरटी, नई दिल्ली

सुश्री शीतल मिश्रा, प्रोजेक्ट इंजीनियर, आईईएसए, सी-डैक, हैदराबाद

साइबर जगत में सुरक्षा

प्रौद्योगिकी ने क्षेत्रीय एवं राष्ट्रीय बाधाओं को दूर करके हमें इस तरह से साथ ला दिया है जिसकी 20 वर्ष पहले तक कल्पना भी नहीं की जा सकती थी। हाल के वर्षों में हमारी सभ्यता की महानतम उपलब्धियाँ प्रौद्योगिकीय सफलताओं से ही हासिल हुई हैं। हालांकि, हर सिक्के के दो पहलू होते हैं। उपलब्धियों के साथ-साथ, साइबर जगत छात्रों के संदर्भ में खतरनाक भी हो सकता है। कुछ छोटी-छोटी गलतियाँ भी बच्चों को बड़े खतरे में डाल सकती हैं। 'ऑनलाइन सुरक्षा' का उल्लेख एवं पालन उन छात्रों के लिए आवश्यक है जो इंटरनेट का प्रयोग करते हैं।
ऑनलाइन सुरक्षा केवल निम्नलिखित मात्र नहीं है।

प्रायः शिक्षक अपने विद्यार्थियों को 'सुरक्षित' रखने के लिए इन निर्देशों का उपयोग करते हैं। परन्तु ऑनलाइन सुरक्षा इससे कहीं अधिक व्यापक है।

एक प्रसिद्ध उक्ति है: ''किसी व्यक्ति को एक मछली देकर आप उसे केवल दिनभर का भोजन देते हैं जबकि किसी व्यक्ति को मछली पकड़ना सिखाकर आप उसे जीवनभर का भोजन देते हैं।''

इसी तरह, ब्लॉक करने या प्रतिबंध लगाने के बजाय, विद्यार्थियों को ऑनलाइन सुरक्षित रहने का ज्ञान और वेब पर सर्फिंग करते हुये अच्छे आचरण का पालन सिखाना ज़्यादा लाभदायक है।

1

तकनीकी पक्ष

क्या करें और क्या न करें

1. इंटरनेट पर जानकारी खोजते समय सुरक्षित खोज विकल्पों (सेफ़ सर्च) का उपयोग करें और साझा करने या अग्रेषित करने से पहले तथ्यों की समुचित जाँच करें।

2. ऑनलाइन बैंकिंग, खरीददारी या भुगतान करते समय, सुनिश्चित कर लें कि वह वेब एड्रेस https:// से शुरू होता हो। यहाँ यूआरएल में 's' सुरक्षा का प्रतीक है। एड्रेस बार में वेब एड्रेस के बाईं ओर 'लॉक आइकॉन' या 'ग्रीन एड्रेस बार' उस वेबसाइट के सुरक्षित होने का प्रतीक है।

3. विभिन्न ऑनलाइन अकाउंट्स के लिए एक ही पासवर्ड का उपयोग न करें।

4. इंटरनेट पर अपने विभिन्न एकाउंट के लिए एक सुरक्षित और अनूठे (यूनीक) पासवर्ड का उपयोग करें जिसमें संख्या, अपरकेस, लोअरकेस, और स्पेशल कैरेक्टर का संयोजन हो।

5. अपने व्यक्तिगत और अधिकारिक प्रयोजनों के लिए अलग-अलग ई-मेल खातों का उपयोग करें। सोशल मीडिया साइट्स के लिए कभी भी अपने अधिकारिक ई-मेल पते का इस्तेमाल न करें।

6. इंटरनेट पर खरीदारी या बैंकिंग के लिए और अपने सोशल मीडिया प्रोफाइल में लॉग-इन करने के लिए सार्वजनिक एवं असुरक्षित वाई-फाई के उपयोग से बचें।

1 तकनीकी पक्ष

7. अपने ऐसे ऑनलाइन एकाउंट्स को हटा दें जो आपके उपयोग में नहीं हैं।

8. किसी भी सॉफ्टवेयर को केवल विश्वसनीय स्रोतों से ही डाउनलोड/इन्स्टाल करें। हमेशा फाइलों को खोलने से पहले स्कैन करें।

9. एड्रैस बार में सीधे यूआरएल टाइप करके ही अपने बैंक की वेबसाइट खोलें, न कि सर्च इंजिन में। ई-मेल या टेक्स्ट संदेश मे दिये लिंक्स को कभी न खोलें।

10. कभी भी अवांछित, अनपेक्षित ई-मेल से आए लिंक या डाउनलोड अटैचमेंट पर क्लिक न करें, चाहे ऐसे ई-मेल ज्ञात स्रोत से आए दिखाई देते हों।

11. सभी महत्वपूर्ण फाइलों का लोकल/क्लाउड स्टोरेज पर नियमित बैकअप लें।

12. वेबसाइटों पर ''कीप मी लॉग इन'' या ''रिमेम्बर मी'' विकल्पों पर क्लिक न करें और सभी खातों को प्रयोग के उपरांत लॉगआउट कर दें।

13. किसी भी व्यक्तिगत जानकारी जैसे नाम, जन्मतिथि, पता आदि का उपयोग कभी भी अपने पासवर्ड के रूप में न करें।

14. कभी भी फोन, ई-मेल या एसएमएस पर अपने व्यक्तिगत/बैंक डिटेल्स को साझा न करें, चाहे कॉलर/प्रेषक परिचित लगता हो।

15. पॉप-अप और संदिग्ध सर्वेक्षणों से दूर रहें। क्लिक करने से पहले सोचें। कंटैंट को ठीक से पढ़ें और सेटिंग्स के माध्यम से सभी अवांछनीय पॉप-अप को बंद करें।

16. केवल जिज्ञासा-मात्र के लिए अनुचित वेबसाइटों या उन वेबसाइटों पर न जाएं जिनसे आप पूरी तरह परिचित न हों।

17. वेबसाइट और वेब ब्राउजर पर अपनी क्रेडिट/डेबिट कार्ड की जानकारी सेव न करें।

1

तकनीकी पक्ष

18. सुरक्षित वाई-फाई नेटवर्क (एसएसआईडी - SSID) पर ही इंटरनेट का उपयोग करें।

19. ऑनलाइन एकाउंट्स में लॉग-इन प्रक्रिया को 'दोहरा या मल्टी-लेवल' रखें।

20. जब ओटीपी, स्मार्ट कार्ड, पिन या आपके द्वारा चुना गया सुरक्षा चित्र आदि अन्य विकल्प के रूप में उपलब्ध हों तो लॉग-इन के लिए यूज़रनेम और पासवर्ड का उपयोग न करें।

21. पासवर्ड की सूची बनाकर अति-सुरक्षित स्थान पर रखें और उन्हें कम से कम त्रैमासिक बदलें।

22. सुनिश्चित करें कि कंप्युटर में नवीनतम सुरक्षा पैच हो और ब्राउज़र, ऑपरेटिंग सिस्टम व एंटीवायरस अप-टु-डेट हों।

23. यह न समझें कि वायरस का पता लगाने वाला सॉफ्टवेयर सदैव कंप्युटर के साथ काम करता है। सिस्टम स्कैन को हमेशा प्राथमिकता दें।

24. क्लाउड स्टोरेज सिस्टम में गोपनीय डेटा को साझा/अपलोड न करें।

25. ऑनलाइन किए गए सभी लेनदेन का रिकार्ड रखें और अपने बैंक खाते की नियमित रूप से जाँच करें।

26. कंप्युटर-सहायक उपकरणों को संरक्षित करने के लिए एक डोमेन नेम सिस्टम (डीएनएस) सेवा जोड़ें।

1

तकनीकी पक्ष

27. जब आप अपने कंप्युटर/टैबलेट/फोन का उपयोग कर चुके हों तो उनकी स्क्रीन को लॉक कर दें या स्वतः लॉक होने के लिए सेट करें।

28. यह न समझें कि आपके डेटा को बनाए रखना और उसकी सुरक्षा करना किसी और की जिम्मेदारी है।

29. ई-मेल को खोलने से पहले सुनिश्चित कर लें कि उसका 'स्रोत हैडर' वैध पते से है।

30. उन दुर्भावनापूर्ण वेबसाइटों के लिंक पर क्लिक न करें जो आपके कंप्युटर में मालवेयर/वायरस लोड कर सकती हैं।

31. स्पैम ई-मेल को बिना सोचे-समझे न खोलें। स्पैम बॉक्स को समय-समय पर जाँचते और खाली करते रहें।

32. चर्चा मंचों/चैट कक्षों पर दूसरों के साथ बातचीत करते हुए सुनिश्चित करें कि कैप्स लॉक कुंजी बंद है क्योंकि बातचीत के दौरान टाइपिंग के रूप में बड़े अक्षरों को असभ्य माना जाता है।

33. विद्यार्थियों द्वारा डिवाइस के उपयोग की निगरानी करें एवं उपकरणों पर बिताए जाने वाले समय को नियंत्रित करें।

34. इंटरनेट या साइबर उपकरणों के प्रयोग में नियंत्रित (पेरंटल लॉक) या छात्र-अनुकूलित प्रोफाइल बनाएं- ब्राउज़र, खोज, वीडियो साइट आदि पर उपलब्ध विकल्पों का उपयोग करें।

35. सुनिश्चित करें कि विद्यार्थियों की पहुँच अनुमति प्राप्त साइट्स/सामग्री तक ही है।

36. बच्चों के इंटरनेट उपयोग की ब्राउजिंग हिस्ट्री की नियमित समीक्षा करें।

2

नैतिक पक्ष

क्या करें और क्या न करें

1. जानबूझकर दूसरों की जानकारी, जिसमें पासवर्ड, फाइलें आदि शामिल हो सकती हैं, को रिकवर या संशोधित करने के लिए कंप्युटर/इंटरनेट का उपयोग न करें।
2. इंटरनेट से साहित्यिक चोरी (Plagiarism) न करें जैसे किसी संसाधन की कॉपी बनाना (पुस्तक, संगीत, वीडियो, सॉफ्टवेयर आदि) क्योंकि यह बेईमानी है और अवैध भी हो सकती है। आप कॉपीराइट कानूनों का उल्लंघन कर सकते हैं।
3. यदि आप किसी सामग्री का उपयोग करना चाहते हैं तो मूल-निर्माता से अनुमति प्राप्त करें। हमेशा संसाधन के मूल-स्वामी को मान्यता और श्रेय प्रदान करें।
4. लोगों के साथ ऑनलाइन बातचीत करते हुए कभी भी नकली पहचान न दें।
5. यदि स्वामित्व अधिकार अनुमति न दें तो दूसरों की मूल रचनाओं से लाभ न कमाएं।
6. सामग्री का उपयोग संसाधन का संदर्भ देकर किया जा सकता है। जब भी संभव हो तो भावानुवाद करें।

3 सामाजिक पक्ष

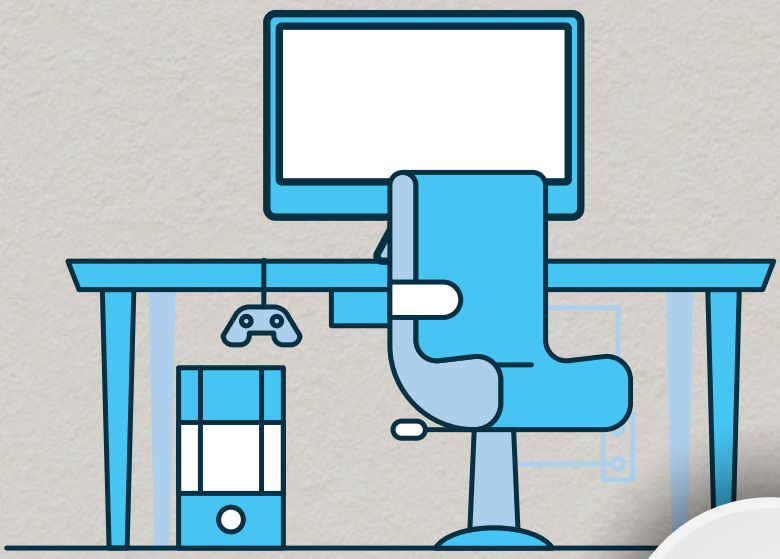
1. सामान्य रूप से सोशल मीडिया और इंटरनेट साइटों पर अपनी निजी जानकारी साझा करने से बचें।
2. गाली - गलौच, अभद्रता, धमकी या अपमानजनक भाषा आदि से साइबर बुलिंग न करें।
3. साइबर बुलिंग करने वालों के साथ न उलझें और न ही बहस करें क्योंकि यह इससे भी बुरे व्यवहार को बढ़ावा दे सकता है।
4. साइबर बुलिंग करने वालों द्वारा भेजे गए ई-मेल या इंस्टेंट संदेश के माध्यम से उत्पीड़न को रोकने के लिए उपलब्ध तकनीकी फिल्टरों का उपयोग करें।
5. उन लोगों से मिलने में सावधानी बरतें जिन्हें आपने केवल ऑनलाइन माध्यम से जाना है।
6. ऑनलाइन कुछ भी ऐसा न करें जो दूसरों की उपस्थिति में करना पसंद न किया जाए।
7. विद्यार्थियों के व्यवहार, अभिवृत्ति, रुचियों में परिवर्तन पर निगरानी रखें और उनसे संवाद स्थापित करें।

4

कानूनी पक्ष

क्या करें और क्या न करें

1. साइबर बुलिंग की सूचना संबन्धित अधिकारियों को दें। किसी साइबर बुली से प्राप्त प्रत्येक टिप्पणी को आगामी कार्यवाही हेतु रेकॉर्ड में रखें।
2. कभी भी ऐसी ई-मेल पर भरोसा न करें जो ऐसी लॉटरी की पुरस्कार राशि प्रदान करता है जिनमें आप प्रतिभागी नहीं है। इसी तरह उन कार्यों के लिए भुगतान न करें, जिनके लिए आपने अधिकारिक चैनलों के माध्यम से पत्राचार नहीं किया है।
3. किसी साइट पर सिर्फ इसलिए भरोसा न करें क्योंकि वह सिर्फ सुरक्षित होने का दावा करती है। वह एक 'फिशिंग' साइट भी हो सकती है।
4. ई-मेल 'स्पूफिंग' से सावधान रहें।
5. ऑनलाइन खरीद का प्रचार करने वाले नकली विज्ञापनों से सावधान रहें।
6. अनाधिकृत व्यक्तियों/डीलरों से कोई भी उपकरण न खरीदें।
7. कभी भी किसी और के ई-मेल को न पढ़ें, भले ही आप उसका पासवर्ड जानते हों।



कानूनी पक्ष

क्या करें और क्या न करें

4

8. कंप्युटर स्रोत, सॉफ्टवेयर के मूल रेकॉर्ड के साथ कभी छेड़छाड़ न करें।
9. बिना व्यक्ति/संगठन की अनुमति के एकत्र किए गए डेटा को कभी भी साझा या परिवर्तित न करें।
10. कभी भी किसी व्यक्ति की तस्वीर को उसकी सहमति के बिना न तो कैप्चर करें, न ही पुनः बनाएं या प्रसारित करें।
11. अनुचित सामग्री को कभी भी प्रकाशित या प्रसारित न करें।
12. बच्चों से संबंधित किसी भी आपत्तिजनक या अपमानजनक इलेक्ट्रॉनिक सामग्री की रिपोर्ट संबंधित अधिकारियों को करें।
13. किसी को भी धमकी भरा, अपमानजनक या अभद्र ई-मेल न भेजें।
14. संस्थान से संबंधित किसी भी कंप्युटर हार्डवेयर एवं अन्य उपकरणों का दुरुपयोग न करें।
15. कॉपीराइट अधिकारों वाले संसाधनों के कानूनी पक्ष का ध्यान रखें।

साइबर कानून

धारा	अपराध	दंड
67A	कामुकता व्यक्त करने वाले कार्य आदि वाली सामग्री के इलेक्ट्रॉनिक रूप में प्रकाशन के लिए	सात वर्ष तक कारावास या 10,00,000 रू तक जुर्माना या दोनों
67B	कामुकता व्यक्त करने वाले कार्य (चाइल्ड पॉर्न) आदि में बालकों को चित्रित करने वाली सामग्री को इलेक्ट्रॉनिक रूप में प्रकाशित या प्रेषित करने के लिए	पहला अपराध सिद्ध होने पर10,00,000 रू तक जुर्माने के साथ 5 वर्ष तक कारावास, दूसरे अपराध पर 7 वर्ष तक कारावास या 10,00,00 रू का जुर्माना या दोनों
67C	मध्यवर्तियों द्वारा सूचना का परीक्षण और प्रतिधारण	3 वर्ष तक कारावास या 2,00,000 रू तक का जुर्माना या दोनों
68	आदेशों के अनुपालन में असफलता/इंकार	7 वर्ष तक कारावास और जुर्माना
69	डाटा डिक्रिप्ट करने में असफलता/इंकार	3 वर्ष तक कारावास या/और 1,00,000 रू तक का जुर्माना या दोना
70	किसी संरक्षित सिस्टम तक पहुंच प्राप्त करना अथवा पहुँच प्राप्त करने का प्रयास करना	10 वर्ष तक कारावास या जुर्माना या दोनों
71	गलत प्रस्तुति या तथ्य छिपाने के लिए	3 वर्ष तक कारावास या/और 1,00,000 रू तक का जुर्माना या दोनों


CYBER SECURITY
MAJOR THREATS
PROTECTING
SAFE PRACTICE
Cyber Crime
Cyber Bullying
Online Predators
Modification
Destruction
Curiosity
Money
Pornography
Slander
False Accusations
Websites
Insults
Teasing
Name Calling
Sexual Activities
Unauthorised Access
Revenge
Fake Account
Libel
IM
Lies
Rumors
Threats
Threats
Grooming
Disruption
Attention
Defamation
E-mails
Disclosure
Fun
Identity Theft
Cyber Stalking
Repeated Harassment
Phone
Online Groups
Harassments
Use/Misuse
Theft
Information & Devices
Share
Changed
Securely
Strong
Password
Morphing
E-Mail Bombing
Website Defacement
Spam
Piracy
Spyware
Virus
Scareware
Social Engineering
Websites Spoofing
Hoax
Malware
Ransomware
E-mail Spoofing
Scam
Hacking
Worms
Click jacking
Phishing
Trojans
Adware
Tab Napping
Copyright Violation
Before Discarding
Authorised Store
Sensitive Information
Phone Call
Instant Messaging
Password
User Name
Credit Card Details
Firewall
Password
Software
Data
Pirated Software
Operating System
Scan
Latest Browser
Content Filtering
Friendship
Cyber Laws
WiFi
E-mail Tracer
Internet
Browser Pluggins
Unknown People Online
Mobile Devices
Auto Lock
Authorised WiFi
IMEI Number
Bluetooth
When Needed
Social Media
Threats
URL
Untrusted Website
Meeting in Person
Call from Weired Number
Call back
Referral Links
E-mail Attachments
Spy Camera
Be Scared
Chat Screen
Cyber Police
Parents
Strangers
Personal Informtion
Privacy Options
Security Options
User to be Old Enough
browser's cookies and cache
Unknown Persons
Type the URL
CC:BY:SA-M.U.Paily

विद्यया ऽ मृतमश्नुते
एन सी ई आर टी
NCERT

केन्द्रीय शैक्षिक प्रौद्योगिक संस्थान
राष्ट्रीय शैक्षिक अनुसंधान और प्रशिक्षण परिषद्
श्री अरविंद मार्ग, नई दिल्ली - 110016

अधिक जानकारी के लिए

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