साइबर जगत में सुरक्षा

विद्यालयों के लिए आवश्यक दिशा-निर्देश

विद्यया ऽमृतमश्नुते

एन सी ई आर टी
NCERT

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, आईइएसए, सी-डैक, हैदराबाद

साइबर सुरक्षा, सूचना एवं संचार प्रौद्योगिकी का सुरक्षित और ज़िम्मेदार उपयोग है। यह सूचना को सुरक्षित बनाए रखने के बारे में तो है ही, साथ ही यह सूचना के प्रति उत्तरदायी होने, ऑनलाइन जगत में अन्य लोगों के सम्मान, और अच्छे नेटिकेट (इंटरनेट शिष्टाचार) का व्यवहार प्रदर्शित करने के बारे में भी है।

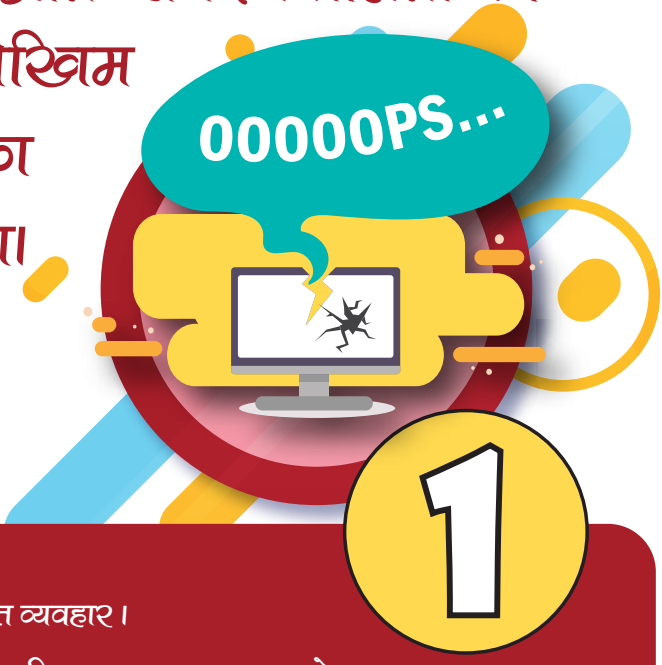
जैसे-जैसे सूचना जगत में आधारभूत संरचना और इंटरनेट अधिक जटिल व विस्तृत हुए हैं, साइबर संसाधनों का उचित प्रबंधन एवं सुरक्षित क्रियान्वयन महत्वपूर्ण हो गया है। यद्यपि हाल के वर्षों में सिस्टम एडमिनिस्ट्रेशन का कार्य आसान हो गया है, फिर भी विद्यालय प्रशासकों को कंप्युटर सिस्टम और नेटवर्क सुरक्षा पर अधिक अपडेट होना चाहिए।

हाल के वर्षों में, सभी कंप्युटर सिस्टम इंटरनेट के संपर्क में आ गए हैं इसलिए इनके सुरक्षित रख-रखाव और हैकर से सुरक्षा चुनौतियाँ बढ़ गई हैं। अतः साइबर हमलों से बचाव सभी शिक्षण संस्थानों की प्राथमिकता होनी चाहिए।

इंटरनेट सुरक्षा के प्रसार एवं इसे सुनिश्चित करने में विद्यालय की मुख्य भूमिका है। 'सिस्टम, कंप्युटर, नेटवर्क उपकरणों' को सुरक्षित और सुचारु रखने के लिए विद्यालय ही प्राथमिक रूप से उत्तरदायी है। संस्थान द्वारा सूचना को सुरक्षित रखना उतना ही आवश्यक है जितना कंप्युटर सिस्टम और नेटवर्क उपकरणों को रखा जाता है।

क्रम सूची

खतरों के प्रति अति-संवेदनशीलता की पहचान और जोखिम की संभावना का आकलन करना।



- सिस्टम का धीमा और सुस्त व्यवहार।
- काम करते समय सिस्टम स्क्रीन का अकारण गायब हो जाना।
- अप्रत्याशित पॉप-अप या असामान्य त्रुटि संदेश।
- अपेक्षित अवधि से पहले कंप्युटर सिस्टम की बैटरी का समाप्त हो जाना।
- कुख्यात बीएसओडी (ब्लू स्क्रीन ऑफ डैथ) का प्रकट हो जाना।
- कार्यक्रमों / प्रणाली का ध्वस्त हो जाना।
- अपडेट, डाउनलोड करने में असमर्थता।
- बिना किसी इनपुट के नए ब्राउजर होम पेज, नए टूलबार अथवा/और अवांछित वेबसाइटों पर नेविगेशन हो जाना।
- आपकी ई-मेल आईडी से दूसरों को असामान्य संदेश चले जाना।
- डेस्कटॉप पर नए, अपरिचित आइकन का प्रकट हो जाना।
- असामान्य संदेश या सॉफ्टवेर प्रोग्राम की उपस्थिति का स्वतः शुरू हो जाना।
- टास्क मैनेजर में चल रहे अनजान कार्यक्रम।

2

जोखिम की पहचान और सुरक्षा उपायों का विकास करना

- एक सक्षम फायरवॉल में निवेश करना।
- सभी द्वारा सुरक्षित और मजबूत पासवर्ड बनाना।
- पासवर्ड मापदंड ऐसा रखें जो मजबूत पासवर्ड दिशानिर्देशों का पालन करता हो।
- पासवर्ड को नियमित रूप से बदलें एवं पुराने पासवर्ड के पुनः उपयोग से बचें।
- केवल सत्यापित ओपन-सोर्स या लाइसेंस प्राप्त सॉफ्टवेर और ऑपरेटिंग सिस्टम का उपयोग करें।
- सुनिश्चित करें कि केवल अधिकृत कर्मियों को ही कंप्युटर सिस्टम और प्रयोगशाला सुलभ हो।
- नेटवर्क पर व्यक्तिगत उपकरणों के उपयोग को हतोत्साहित करें, जैसे कि व्यक्तिगत यूएसबी या हार्डड्राइव।
- अपने कंप्युटर पर साफ्टवेयर और आपरेटिंग सिस्टम की स्वचालित अपडेट विचार करके ही स्थापित करें।
- कंप्युटर सिस्टम में एंटीवायरस को नियमित रूप से अपडेट करें।
- कंटैंट फिल्टरिंग सॉफ्टवेयर/फ़ायरवाल का उपयोग करते हुये फाइल-फ़ारमैट जैसे- .bat .cmd .exe .pif आदि को ब्लॉक करने पर विचार करें।

जोखिम की पहचान और सुरक्षा उपायों का विकास करना

2

- किसी सॉफ्टवेयर को सिस्टम पर स्थापित करने से पूर्व उसके वैध लाइसेंस को पढ़ लें कि वह हानिकारक एडवेयर और स्पाइवेयर तो इन्स्टाल नहीं कर रहा।
- इंटरनेट के माध्यम से ऑफिस या विद्यालय कंप्युटर नेटवर्क की रिमोट एक्सेस के लिए एसएसएल या वीपीएन जैसे एनक्रिप्शन का उपयोग करें।
- सुनिश्चित करें कि तीसरे पक्ष के विक्रेताओं, जिनका विद्यालय के साथ अनुबंध है, उन्होंने मजबूत सुरक्षा व्यवस्था स्थापित की है।
- नेटवर्क की सुरक्षा के लिए विश्वसनीय, सत्यापित तृतीय-पक्ष विक्रेता के साथ ही अनुबंध करने पर विचार करें।
- विद्यालय के नेटवर्क पर लॉग-ऑन करते समय दो या बहुकारक (पासवर्ड, कैपचा, ओटीपी आदि) प्रमाणीकरण संस्थापित करें।
- अपने वाई-फाई कनैक्शन को मजबूत पासवर्ड, WEP एनक्रिप्शन आदि से संरक्षित रखें।
- एनक्रिप्शन आधारित नेटवर्क ट्रैफिक को प्राथमिकता दें।
- डिफॉल्ट पासवर्ड को प्रथम लॉग-इन के समय सुरक्षित पासवर्ड में अवश्य बदलें। अगर वायरलैस नेटवर्क में कोई डिफ़ाल्ट पासवर्ड नहीं है तो नया बनाएं और नेटवर्क के संरक्षण के लिए इसका उपयोग करें।
- संस्थान के नेटवर्क पर फ़ाइल-शेयरिंग की अनुमति आवश्यकता अनुसार ही दें।
- नेटवर्क लंबे समय तक उपयोग में ना हो तो उसे बंद कर दें।
- विद्यार्थियों को हानिकारक सामग्री/वैबसाइट तक पहुँचने से रोकने के लिए कुछ उपायों जैसेः रेस्ट्रिक्टेड मोड, सेफ़-सर्च, सुपरवाइज्ड यूजर्स और सामान्य फ़िल्टर्स तथा निगरानी प्रणाली का उपयोग करें, जिससे साइबर खतरों का शीघ्र पता चल सके।

3

संवेदनशील डेटा की सुरक्षा करना

- कंप्युटर स्टोरेज एक्सेस (प्रयुक्त/अप्रयुक्त), सुरक्षा एवं बचाव के मूल्यांकन पर आधारित सुरक्षा और अभिगम नियंत्रण को डिजाइन और लागू/अमल करें।
- कंप्युटर सिस्टम की सी-ड्राइव में महत्वपूर्ण जानकारी/फाइल्स संग्रहीत न करें।
- किसी ऑफ-साइट स्थान पर महत्वपूर्ण डेटा (मोबाइल नंबर, आधार संख्या आदि) का बैकअप लें।
- रिपोर्ट करने वाले व्यक्ति की पहचान के संरक्षण के लिए सुरक्षित रिपोर्टिंग दिशानिर्देशों और त्वरित कार्यवाही के तरीकों को स्थापित करें।

4 साइबर सुरक्षा घटनाओं का आकलन करना और इनसे उबरना

- **प्रारंभिक आकलन:** उचित प्रतिक्रिया सुनिश्चित करने के लिए यह आवश्यक है कि प्रतिक्रिया टीम निम्नलिखित पर ध्यान दे:
  - घटना कैसे हुई ?
  - कौन से आईटी और/या ओटी (Operational Technology) सिस्टम इससे प्रभावित हुए और कैसे?
  - डेटा किस सीमा तक प्रभावित हुआ?
  - आईटी और ओटी के लिए खतरा किस सीमा तक विद्यमान है?

- **सिस्टम और डेटा की पुनः स्थापना:** साइबर घटना के प्रारंभिक आकलन के पश्चात सिस्टम से खतरों को हटाकर आईटी एवं ओटी सिस्टम और डेटा की यथासंभव पुनः स्थापना करके उसे कार्य करने की स्थिति में ले आना चाहिए।

- **घटना की जांच करें:** किसी साइबर घटना के कारणों और परिणामों को समझने के लिए यदि उपयुक्त हो तो कंपनी के द्वारा एक बाहरी विशेषज्ञ के सहयोग से जांच की जानी चाहिए। ऐसी जाँच से मिली जानकारी संभावित पुनरावृत्ति को रोकने में महत्वपूर्ण भूमिका निभाएगी।

- **पुनरावृत्ति को रोकें:** ऊपर उल्लेखित जांच के परिणाम को ध्यान में रखते हुए तकनीकी और प्रक्रियात्मक सुरक्षा उपायों में किसी भी अपर्याप्तता का सामना करने के लिए कंपनी सुधारात्मक कार्यवाही के क्रियान्वयन के लिए प्रक्रियाओं के अनुसार कार्यवाही पर विचार किया जाना चाहिए।

5

हितधारकों को प्रशिक्षित करना

- विद्यालय के लिए "क्या करें, क्या न करें" के रूप में साइबर सुरक्षा नियमों का संयोजन करें।
- विद्यालय प्रशासकों को नवीनतम उपकरणों के बारे में जागरूक करें जिनका उपयोग विद्यार्थियों/ शिक्षकों द्वारा देखी गई साइटों की निगरानी के लिए किया जा सके।
- साइबर कानूनों के विषय में हितधारकों को जागरूक करें (https://mha.gov.in/sites/default/files/CyberSafety_English_Web_03122018.pdf)
- साइबरस्पेस में जोखिमों और इनके निवारक उपायों के बारे में जागरूकता के स्तर को बढ़ाने के लिए साइबर सुरक्षा विशेषज्ञों से विमर्श करें।
- साइबर सुरक्षा और बचाव के प्रमुख घटकों पर छात्रों और शिक्षकों को पाठ्यक्रम/पाठ/ कार्यकलापों से परिचित कराएं।
- डिजिटल सूचना एवं प्रौद्योगिकी के सुरक्षित, वैध और नैतिक उपयोग की वकालत करें, आदर्श स्थापित कर प्रेरित करें।
- प्रौद्योगिकी और सूचना के उपयोग से एक आदर्श एवं उत्तरदायी सामाजिक सहभागिता को बढ़ावा दें।
- साइबर क्लबों के माध्यम से जागरूकता पैदा करने के लिए साइबर सुरक्षा सप्ताह/उत्सव मनाएं और संबन्धित गतिविधियों का संचालन करें।
- किसी प्रतिष्ठित साइबर सुरक्षा फर्म/संगठन के साथ संबंध स्थापित करें।
- साइबर जगत में विद्यालय के हितों को सुरक्षित रखने के लिए निर्देशों, नीतियों और प्रक्रियाओं का पालन करें।

www.ictcurriculum.gov.in

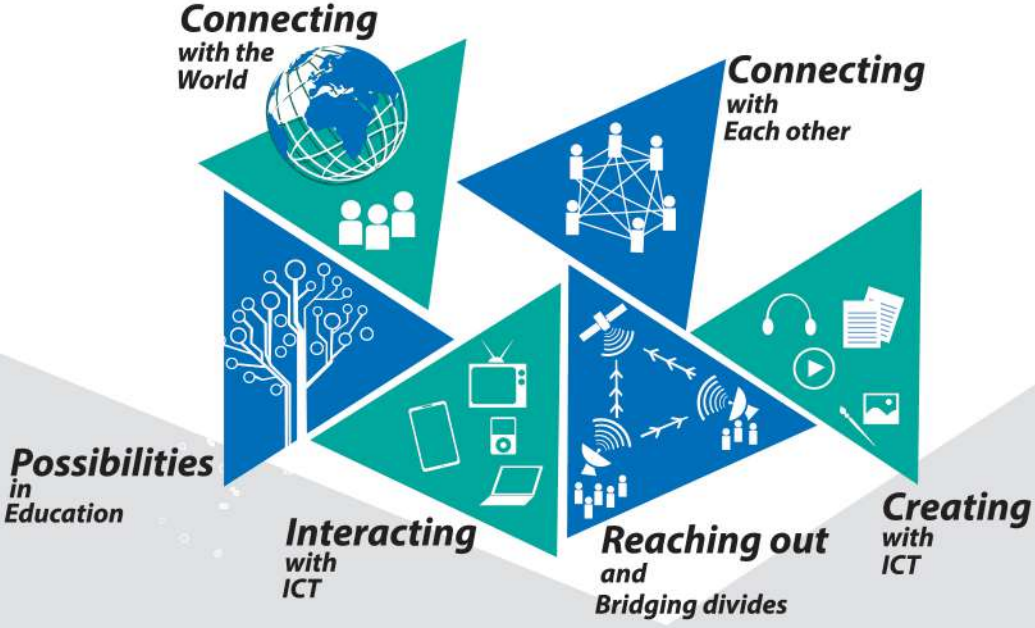
Curricula for Information and Communication Technology (ICT) in Education

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 critically interact with information.

The Curricula is organised into six strands:




CYBER SECURITY
MAJOR THREATS
PROTECTING
SAFE PRACTICE
means
Cyber Crime
include
from
committed
for
Modification
Destruction
Curiosity
Money
Pornography
Unauthorised Access
Revenge
Fake Account
Disruption
Attention
Disclosure
Information & Devices
Fun
Identity Theft
Use/Misuse
Theft
Slander
False Accusations
Libel
Defamation
including
is
Cyber Stalking
Repeated Harassment
through
Websites
IM
E-mails
Phone
Online Groups
Cyber Bullying
Insults
Teasing
Name Calling
Lies
Rumors
Threats
Online Predators
Threats
Sexual Activities
Grooming
Harassments
Morphing
E-Mail Bombing
Website Defacement
Spam
Piracy
Hoax
Malware
Scam
Hacking
Phishing
Copyright Violation
Spyware
Virus
Scareware
Ransomware
Trojans
Worms
Adware
uses
Social Engineering
obtaining
Sensitive Information
Websites Spoofing
E-mail Spoofing
Click jacking
Tab Napping
Instant Messaging
Phone Call
like
Password
User Name
Credit Card Details
Share
Changed
should be
do not
Password
save
Securely
Strong
shoud be
use
Firewall
protect
Password
Software
update
Desktop/ Laptop
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
ensure
Privacy Options
Security Options
User to be Old Enough
Latest Browser
Content Filtering
WiFi
secure
E-mail Tracer
Internet
Friendship
with
Unknown People Online
avoid
Meeting in Person
Browser Pluggins
Untrusted Website
never visit
any
Threats
check
URL
inform
Parents
approach
Cyber Police
save
Chat Screen
do not
Be Scared
beware of
Spy Camera
clean
browser's cookies and cache
do not open
E-mail Attachments
from
Unknown Persons
Referral Links
instead
Type the URL
in using
Mobile Devices
format
Before Discarding
download app from
Authorised Store
do not accept
Call from Weired Number
and do not
Call back
use
Auto Lock
access only
Authorised WiFi
record
IMEI Number
switch on
Bluetooth
only
When Needed
CC:BY:SA-M.U.Paily

अधिक जानकारी के लिए

www.ciet.nic.in
www.ictcurriculum.gov.in
www.infocyberawarness.com
www.ncert.nic.in

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