

Cyber Safety and Security

Guideline for School

विद्यया ऽ मृतमश्नुते



एन सी ई आर टी
NCERT



Be safe in cyber world ...

Curricula for Information and Communication Technology (ICT) in Education

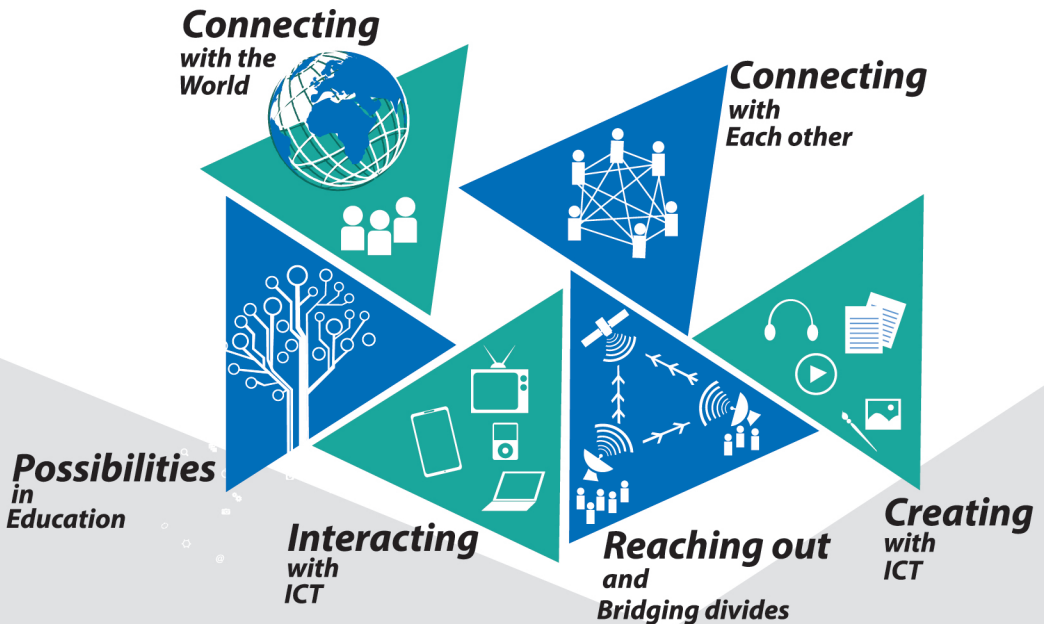


सत्यमेव जयते

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:



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

Members:

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

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.



Cybersafety is the safe and responsible use of information and communication technology. It is about keeping information safe and secure, but also about being responsible with that information, being respectful of other people online, and using good 'netiquette' (internet etiquette).

As information infrastructure and Internet became more complex and larger, it also became critical to maintain systems up and running all the time with respect to security. Though the system administration tasks became easier in recent years, school administrators need to be more updated on the systems and network Security they are managing. In recent years, all systems are exposed to Internet; there is increased challenge for maintaining and protecting from the attackers.

Schools are primarily responsible for keeping systems/ computers/ network devices to work smoothly and securely. It is very important to keep the information as much securing the system and network devices in the organization. Schools play a key role in promoting internet safety.

Index

1

Identify threats
vulnerability
and
assess risk exposure

2

Develop protection
and
detection measures

3

Protect
sensitive data

4

Respond to
and recover
from
cyber security
incidents

5

Educate your
stakeholders

Identify threats vulnerability and assess risk exposure

00000PS...

1

- ⦿ Slow and sluggish behavior of the system.
- ⦿ Inexplicable disappearance of system screen while working.
- ⦿ Unexpected popups or unusual error messages.
- ⦿ Drainage of system battery life before expected period.
- ⦿ Appearance of the infamous BSOD (Blue Screen of Death).
- ⦿ Crashing of programs/ system.
- ⦿ Inability to download updates.
- ⦿ Navigation to new browser homepage, new toolbars and/or unwanted websites without any input.
- ⦿ Circulation of strange messages from your email id to your friends.
- ⦿ Appearance of new , unfamiliar icons on Desktop.
- ⦿ Appearance of unusual message or programs which start automatically.
- ⦿ Unfamiliar programs running in Task Manager.



2

Develop protection & detection measures

- ◉ Invest in a robust firewall.
- ◉ Have students and teachers create strong passwords.
- ◉ Have a password protocol that specifies strong password guidelines, frequent change of passwords, prevents reuse of old passwords.
- ◉ Use only verified open source or licensed software and operating systems.
- ◉ Ensure that computer systems and labs are accessed only by authorized personnel.
- ◉ Discourage use of personal devices on the network, such as personal USBs or hard drives.
- ◉ Set up your computer for automatic software and operating system updates.
- ◉ Check that antivirus softwares in each system are regularly updated.
- ◉ Consider blocking of file extensions such as .bat, .cmd, .exe, .pif by using content filtering software.



Develop protection & detection measures

2

- ◆ Read the freeware and shareware license agreement to check if adware and spyware are mentioned, before installing them on systems.
- ◆ Use encryption such as SSL or VPN for remote access to office or school lab through internet.
- ◆ Ensure that third-party vendors (who have contract with the school) have strong security measures in place.
- ◆ Consider contracting with a trusted / verified third-party vendor to monitor the security of your school's network.
- ◆ Institute two or multi factor authentication for students, teachers and administrators when they log on.
- ◆ Protect your Wi-Fi Connection with secure password, WEP encryption, etc.
- ◆ Encrypt the network traffic.
- ◆ Change the administrator's password from the default password. If the wireless network does not have a default password, create one and use it to protect the network.
- ◆ Disable file sharing on computers .
- ◆ Turn off the network during extended periods of non-use etc.
- ◆ Use "restricted mode", "safesearch", "supervised users" and other similar filters and monitoring systems, so that no child can access harmful content via the school's IT systems, and concerns can be spotted quickly.



3



Protect sensitive data

- ⑥ Design and implement information security and access control programmes and policies, by evaluating the storage (used/ unused), access, security and safety of sensitive information.
- ⑥ Never store critical information in system's C drive.
- ⑥ Backup critical data (mobile numbers, aadhaar number etc.,) in an off-site location.
- ⑥ Establish safe reporting guidelines and escalation methods to protect the identity the person who reports.

Respond to and recover from cyber security incidents

4



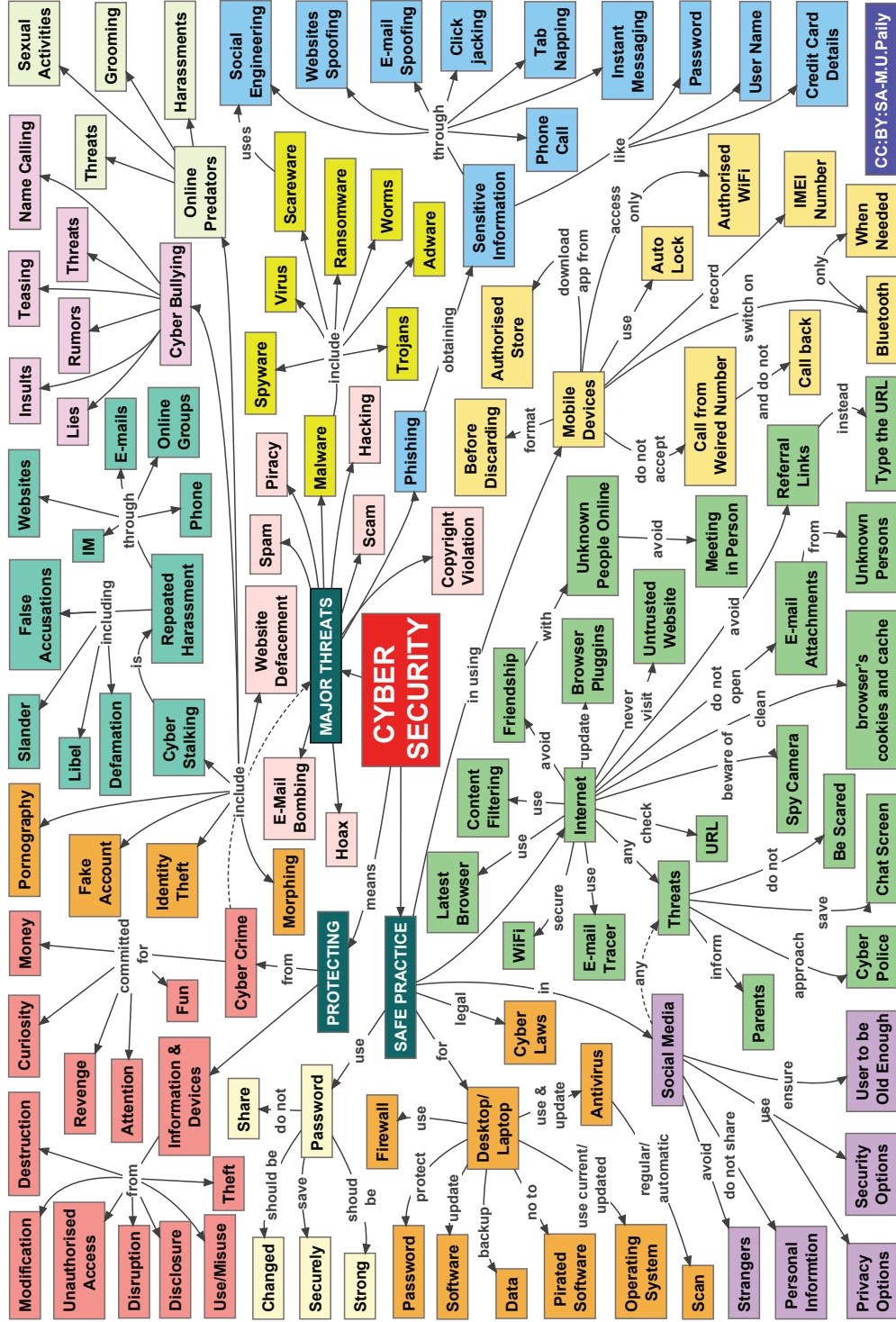
- ◉ **Initial assessment:** To ensure an appropriate response, it is essential that the response team find out:
 - How the incident occurred ?
 - Which IT and/or OT systems were affected and how ?
 - The extent to which the commercial and/or operational data was affected ?
 - To what extent any threat to IT and OT remains ?
- ◉ **Recover systems and data:** Following the initial assessment of the cyber incident, IT and OT systems and data should be cleaned, recovered and restored, so far as is possible, to an operational condition by removing threats from the system and restoring software.
- ◉ **Investigate the incident:** To understand the causes and consequences of a cyber incident, an investigation should be undertaken by the company, with support from an external expert, if appropriate. The information from an investigation will play a significant role in preventing a potential recurrence.
- ◉ **Prevent re-occurrence:** Considering the outcome of the investigation mentioned above, actions to address any inadequacies in technical and/or procedural protection measures should be considered, in accordance with the company procedures for implementation of corrective action.

5

Stakeholders

Educate your stakeholders.

- ◉ Frame cyber safety rules as Do's and Don'ts for the Schools.
- ◉ Orient school administrators with latest tools that can be used to monitor the sites visited by the students/ teachers.
- ◉ Orient the stakeholders on cyber laws (<http://cyberlawsindia.net/>)
- ◉ Bring in cybersecurity professionals to raise awareness levels about the risks in cyberspace and its preventative measures
- ◉ Introduce courses/ lessons/ activities for students and teachers on major components of cyber security and safety.
- ◉ Advocate, model, and teach safe, legal, and ethical use of digital information and technology.
- ◉ Promote and model responsible social interactions related to the use of technology and information
- ◉ Celebrate Cyber Security Week and conduct activities to create awareness through cyber clubs
- ◉ Establish a relationship with a reputable cybersecurity firm/ organisation.
- ◉ Be aware about policies and procedures to keep the school safe and secure in cyberspace.



For more details visit

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



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