

I/6619/2021

Government of Jammu & Kashmir
Directorate of School Education, Jammu

Muthi Jammu, J&K PIN: 181205

No: DSEJ/Counselling/37746-37870

Dated: 23/11/2021

The Chief Education Officers (All)
Jammu Division

Subject: Observance of 'Cyber Jaagrookta Diwas' on first Wednesday of every month.

Ref 1: Communication from Administrative department vide No: Edu-PS00R/98/2021-01(80233) date 11/11/2021

Ref 2: Communication from Headquarters Crime branch J&K vide No: CHO/CICE/15198 dated: 08/11/2021.

Apropos the subject and references cited above, in this context this office has received communication from Administrative department and Headquarters Crime branch J&K regarding implementation of a Scheme called "Indian Cyber-crimes coordination center" (I4C) and to observe '**Cyber Jaagrookta (Awareness) Diwas**' in all schools (6th standard onward for all classes) of Jammu Division till October 2022.

The exponential increase in the number of internet users in India and rapidly evolving technologies have brought in its own unique challenges, besides aggravating the existing problems of cybercrimes, which is one of the fastest growing forms of transnational and insidious crimes.

As you are aware, the Ministry of Home Affairs is implementing a scheme called the 'Indian Cyber Co-ordination Centre (I4C)' to deal with cyber-crimes in a coordinated and comprehensive manner. This Ministry has developed a 'national Cybercrime Reporting Portal' for ease of filling of complaints relating to cyber-crimes by citizens on 'anywhere, anytime' basis.

With a view to strengthen cyber security for prevention of cybercrimes, need has been felt for a multi-pronged strategy involving all stakeholders of School Education Department.

In this regard, you are hereby directed to instruct HOIs (MS, HS, HSS) of all educational institutions. (Both Govt. and Private)

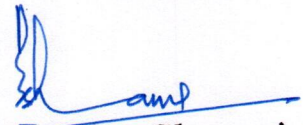
- i. To ensure observance of '**Cyber Jaagrookta (Awareness) Diwas**' in all schools (6th standard onward for all classes) on **first Wednesday** of every month in all schools of Jammu Division for one hour to create awareness for prevention of cybercrimes.
- ii. As a ready reckoner a list of suggestive topics to be taken up for creating awareness among students is enclosed herein for kind perusal and their usage by all stakeholders. (**Annexure "B"**)
- iii. In addition to above, the students may also be informed about "National Cybercrimes Reporting Portal" <https://cybercrimes.gov.in> and a toll free helpline **155260** to assist citizens for registration of complaints on portal. Further, students may also be informed about @Cyberdost twitter handle,

File No. DSEJ-13/38/2021-O/o Lect-JAMMU
 Instagram handle (<https://www.instagram.com/cyberdosti4c>),
 Facebook handle (<https://www.facebook.com/CyberDosti4C>)
 LinkedIn handle (<https://www.linkedin.com/company/cyberdosti4c>) for providing
 regular safety tips related to prevention of cybercrimes.

You are further directed to ask all the HOIs to organize different activities (Short movie screening, Inter-house competition, Symposium, Experience sharing, lectures, Quiz, Slogan writing, Skits etc.) as part of **Cyber Jaagrookta (Awareness) Diwas'** programme.

Find enclosed annual action plan on cyber awareness. (Annexure 'A')

For any related query, call or whatsapp Tele-counselling helpline number 6006800068.


 (Dr. Ravi Shankar Sharma) JKAS
 Director School Education
 Jammu

Copy to:

1. Principal Secretary to Government, School Education Department, Civil Secretariat, Jammu J&K Srinagar for kind information.
2. Spl. Director General of Police, Crime Headquarters J&K Jammu for information and further necessary action.
3. Deputy Director (PD&M) School education Department for information.
4. Joint Directors, School education (Jammu division) for information.
5. Principal DIET(s), Jammu Division for information and necessary action.
6. ZEOs (all) Jammu Division for information and necessary action.
7. Dr. Romesh Kumar, Head Counselling Cell for information and necessary action.
8. IC Website for uploading it on Website.

I/6619/2021

Annual plan on Cyber Awareness.

1. Observance of '**Cyber Jaagrookta Diwas**' on first Wednesday of every month.
2. Inclusion of Cyber awareness themes in **annual counselling calendar** of DSEJ.
3. Conduct of special **PTMs** on Cyber awareness.
4. Conduct of Special Weekly, **fortnightly, Monthly campaigns** Cyber awareness.
5. Publicizing initiatives of I4C through Social media.
6. Publication of **advisories** in newspapers.
7. Conduct of virtual **Panel Discussions** on cyber awareness.
8. Involving other organizations to conduct special sessions.
9. Conduct of Special quiz competitions to assess knowledge about Cyber hygiene.
10. Virtual training through reputed institutes like TISS, Unicef on cyber security etc.
11. Playing Jingles on cyber awareness on radio.
12. Playing scrolls on cyber security through TV channels.
13. Curriculum development on cyber security in collaboration with JK SCERT

Activities to be undertaken

Webinars, Short movie screening, Inter-house competitions, Symposium, Experience sharing, lectures, Quiz, Slogan writing, Skits, Poster making, etc.

I/6619/2021

SUGGESTIVE TOPICS FOR CREATING AWARENESS ARE HIGHLIGHTED BELOW:**FOR PRIMARY STUDENTS OF CLASS 6TH TO 10TH STANDARDS**

- Introduction to cybercrimes.
- Kinds of cybercrime: phishing, identify theft, cyber stalking, cyber obscenity, computer vandalism, ransom ware, identity theft.
- Spotting fake apps and fake news on social media and internet (fake email messages, fake posts, fake what Sapp messages, fake customer care / toll free numbers, fake jobs)
- Internet Ethics, internet addiction, ATM scams, online shopping threats, lottery emails/SMS, Debit/ Credit card fraud, Email security, mobile phone security.
- Mobile apps security, USB Storage Device security.
- Mobile connectivity Security Attacks(Bluetooth , Wi-Fi, Mobile as USB)
- Preventive measures to be taken in Cyber Space, reporting of cybercrime.

FOR STUDENTS OF CLASS 11TH STANDARD AND ABOVE**UNIT -1: CYBER CRIMES AND SAFETY**

- Introduction to cybercrimes
- Kinds of cybercrimes: phishing, identify theft, cyber stalking, cyber obscenity, computer vandalism, Ransom ware, identity theft.
- Forgery and fraud from mobile devices.
- Work on different digital platforms safely.
- Online cybercrimes against women and impersonation scams.
- Safety in Online Financial transaction.

UNIT – II: CONCEPTS AND USE OF CYBER HYGIENE IN DAILY LIFE

- Browser Security, Desktop security, UPI Security, Juice Jacking, GOOGLE Map Security, OTP fraud.
- IOT Security, Wi-Fi Security, Spotting fake apps on social media and internet(fake email messages, fake posts, fake what Sapp messages, fake customer care/ toll free numbers, fake jobs)
- Internet Ethics, internet addiction, ATM scams, online shopping threats, lottery emails/SMS, loan frauds.
- Mobile connectivity security attacks (BLUETOOTH, Wi-Fi) USB storage device security, data security.
- Preventive measures to be taken in cyber space, reporting of cybercrime.

UNIT-III: INTRODUCTION TO SOCIAL NETWORK

- Social network and its contents, blogs.
- Safe and proper use of social networks inappropriate content on social network.
- Flagging and reporting of inappropriate content.

UNIT -1V: ELECTRONIC PAYMENTS AND SAFEGUARD THREAT

- Concept of E- payments, ATM and Tele Banking.
- Immediate payment system, mobile money transfer and E- Wallets.
- Unified Payment interface (UPI).
- Cybercrimes in Electronic Payments.
- KYC: Concept, cases, and suggestions.