



GOVERNMENT OF NATIONAL CAPITAL TERRITORY DELHI
DIRECTORATE OF EDUCATION: SCHOOL BRANCH
OLD SECRETARIAT: DELHI-110054

No. DE.23 (564)/Sch. Br./2021/ 123

Dated: 22/02/2021

CIRCULAR

Sub: Regarding ensuring safety and protection of children from online threats during Covid -19.

The School Education has shifted from the carefree days of learning together in the safe school environment to online mode of gaining knowledge during COVID-19. Hence, it is necessary to ensure the safety of students while they are on internet.

The internet spaces are growing & multiplying and data security, privacy and protection is inadequate to keep a check on this, it is important that everyone is aware of the risks that could be associated with being connected to the internet. In addition, the students need to be warned against these risks and it is extremely important for us to ensure that every possible step is taken towards giving our children safe spaces to learn that keep their innocence and cater to their curiosity in a non-harmful way.

A study has been conducted by India Child Protection Fund (ICPF), New Delhi regarding on-line exploitation of children and increase in activities related to child sexual abuse material (CSAM) which indicates a sharp rise in demand for online child pornography during lockdown. Hence, it is imperative to make children and their parents aware about the safe use of internet.

NCERT and UNESCO have jointly developed guidelines on "SAFE ONLINE LEARNING IN TIMES OF COVID-19" for sensitization of students & parents. The same could be accessed through the below given link:

<https://en.unesco.org/news/mhrd-ncert-and-unesco-bring-attention-counter-cyberbullying>

Copy of the guidelines developed jointly by NCERT and UNESCO is attached herewith.

Therefore, all the Heads of Govt, Govt. Aided, Unaided Private Recognized Schools of Directorate of Education and local bodies i.e. MCDs, NDMCs & Delhi Cantonment Board of Delhi are hereby directed to share this

3/2/21

information with the teachers, students and parents through SMS, Whatsapp Groups or by any other possible means which are being used to reach out to children and parents.

This issues with approval of the Competent Authority.

Attachments: Guidelines for 'Safe Online Learning in times of COVID-19'.


19/02/2021

Dr. Rita Sharma
Addl. DE (School)

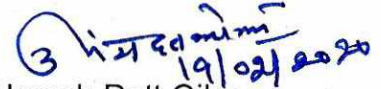
Heads of All Govt, Govt. Aided, Unaided Private Recognized Schools of Directorate of Education and local bodies i.e. MCDs, NDMCs & Delhi Cantonment Board of Delhi through DEL-E.

No.DE.23 (564)/Sch.Br./2021/ 123

Dated: 22/02/2021

Copy to:-

1. PA to Pr. Secretary (Education).
2. PA to Director (Education).
3. Chairperson, NDMC.
4. Director, Education North DMC.
5. Director, Education South DMC.
6. Director, Education East DMC.
7. Director, Education NDMC.
8. Commissioner, Delhi Cantonment Board.
9. All RDEs
10. Sr. Consultant, DCPCR
11. DDEs (District/Zonal) through DEL-E.
12. DDE (ASB/PSB).
13. System Analyst for uploading on the website.
14. Guard File.


19/02/2020
Umesh Datt Ojha
DDE (School)

Why is it important to know about cyberbullying?

Cyberbullying involves the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature and is a punishable offence under the Information Technology Act, 2000 and the Indian Penal Code. It also involves posting pictures or videos aimed at harassing another person. A whole gamut of social platforms, including chat rooms, blogs and instant messaging are used in cyberbullying.

With COVID-19 closing schools across all states, Education Departments have made efforts to ensure continuity of learning through various digital platforms. Millions of learners are turning to online education and with this comes a huge increase in use of electronic devices and Information and communication Technologies (ICTs). This places children and young people at risk of online abuse, increasing their vulnerability to cyberbullying. Cyberbullying is widespread and affects a significant number of children and adolescents and infringes their rights to education and to health and well-being.

There are considerable negative effects of cyberbullying, including on academic achievement, mental health, and quality of life in general. Online bullying often prevents teachers from imparting quality education through digital platforms and acts against the provision of safe, non-violent and inclusive learning environments for all.



Cyberbullying includes



Posting hurtful, nasty rumours or comments on updates, pictures and videos shared by an individual on websites.



Uploading embarrassing photographs online without the person's permission.



Excluding individuals of different cultural, socio-economic backgrounds from online groups and forums.



Stealing someone's account password and sending unwanted/inappropriate messages from that account to harass other individuals.

How to stay safe online?

Do's

- Create a strong password according to password guidelines, and frequently change passwords to prevent misuse.
- Read the privacy settings very carefully on social networking sites.
- Communicate only with known people.
- Be careful while posting photographs, videos and any sensitive information on websites as they leave digital footprints which stay online forever.
- Ensure that only authorized personnel access computer systems and labs.
- Report immediately to the support team of networking site if you suspect that your account have been hacked or stolen.
- Invest in a strong network security system.
- Use only verified open source or licensed software and operating systems.
- Set up your computer for automatic antivirus software and operating system updates.

Don'ts

- Don't reveal your password to anyone other than your parent or guardian.
- Don't reveal personal information like age, address, phone number, school name etc. as this can lead to identity theft.
- Don't post anything which hurts others feelings.
- Don't post your friends' information on networking sites, which can put them at risk.
- Don't forward anything that you read on social media without verifying it from a trusted source.
- Don't leave your account unattended after login, log out when you are not using it.
- Don't create fake profiles for yourself on any social networking site.
- Don't use personal devices such as personal USBs or hard drives on public networks or computers.
- Don't open links and attachment on social networking sites and block file extensions such as .bat, .cmd, .exe, .pif by filtering software.

The law supports you!

Cyberbullying is a punishable offence under the Information Technology Act, 2000 and the Indian Penal Code.

All children and adults MUST report cases of cyberbullying to the police (Dial: 112).



How to prevent and counter cyberbullying?



Do not respond

If someone is bullying you online, DO NOT respond or retaliate by doing the same thing. Responding or retaliating may make matters worse or even get you into trouble.



Collect as much information as possible

Take a screenshot of anything that you think could be cyber bullying and keep a record of it.



Block and report

If someone bothers you, make sure you block the offender and report on the social media platform immediately. This feature is available on most online platforms.



Talk about it

Inform trusted adults like your parents and teachers about the bullying incident. Seek help. Do not feel that you are alone and never keep it to yourself.



Be private

Keep your social media privacy settings high and do not connect with anybody who you do not know offline.



Be aware

Remain updated with all the preventive and security measures in the cyber world.

SUPPORT AND HELPLINE NUMBERS

Police: **Dial 112** (Police has Cyber Crime Cell that handles cases of cybersecurity)

Complaint: **cp.ncpcr@nic.in**
(National Commission for Protection of Child Rights)

Childline Number: **1098**
Complaint: **www.childlineindia.org**

Complaint: **cybercrime.gov.in**
(National Cyber Crime Reporting Portal)
Helpline number: **155260**
Twitter handle: **@CYBERDOST**

Complaint: **complaint-mwcd@gov.in**
(The Ministry of Women and Child Development)

कोविड-19 के दौरान सुरक्षित तरीके से ऑनलाइन माध्यम द्वारा सीखना



सयुक्त रूप से विकसित

साइबर बुलिंग को समझना क्यों आवश्यक है?

साइबर बुलिंग के लिए किसी व्यक्ति का उत्पीड़न करने हेतु इलेक्ट्रॉनिक माध्यम की आवश्यकता होती है, जो कि किसी व्यक्ति को धमकाने या डराने वाले संदेश प्रेषित करके किया जाता है और यह सूचना एवं प्रौद्योगिकी अधिनियम, 2000 एवं भारतीय दंड के तहत दंडनीय अपराध है! इसके अंतर्गत किसी की फोटो या वीडियो भी उसको परेशान करने के लिए पोस्ट किया जाता है। सोशल प्लेटफॉर्म के सभी पहलुओं, जिसमें चैट रूम, ब्लॉग्स, तुरंत संदेश भेजने के माध्यम शामिल हैं, का प्रयोग साइबर बुलिंग के लिए किये जाते हैं।

कोविड 19 की वजह से समस्त राज्यों ने विद्यालयों को बंद कर दिया है, ऐसे में शिक्षा विभाग विभिन्न डिजिटल प्लेटफॉर्म का इस्तेमाल करते हुए सीखने की निरंतरता को बनाए रखने का प्रयास कर रहा है। लाखों की संख्या में विद्यार्थी ऑन-लाइन शिक्षा से जुड़े हैं जिसकी वजह से इलेक्ट्रॉनिक उपकरण एवं सूचना व संचार प्रौद्योगिकी के उपयोग में काफी वृद्धि हुई है। यह युवाओं एवं बच्चों को ऑन-लाइन दुरुपयोग के खतरे में भी डाल रही है साथ ही उनके साइबर उत्पीड़न का शिकार होने की संभावना को भी बढ़ा रही है। साइबर उत्पीड़न बड़े पैमाने पर अच्छी खासी संख्या में बच्चों एवं युवाओं को प्रभावित कर रहा है व उनके शिक्षा, स्वास्थ्य एवं कल्याण के अधिकारों पर कुठाराघात कर रहा है।

साइबर बुलिंग की अच्छी खासी नकारात्मक घटनाएँ हैं, जो कि शैक्षिक उपलब्धि, मानसिक स्वास्थ्य एवं जीवन की गुणवत्ता से संबंधित हैं। ऑनलाइन माध्यम से उत्पीड़ित अध्यापकों को डिजिटल प्लेटफॉर्म के माध्यम से गुणवत्तापूर्ण शिक्षा प्रदान करने में बाधा उत्पन्न करता है और सुरक्षित, हिंसा रहित शिक्षा एवं बच्चों एवं किशोर/किशोरियों के समावेशी सीखने के माहौल के विरोध में कार्य करता है।



साइबर बुलिंग में शामिल हैं



वेबसाइट पर किसी व्यक्ति द्वारा डाले गए अपडेट, फोटो एवं वीडियो पर आहत करने वाले कमेंट या गलत अफवाह पोस्ट करना



किसी व्यक्ति की सहमति के बिना उसकी फोटो डाल कर उसको शर्मसार करना



किसी व्यक्ति को अलग संस्कृति, सामाजिक-आर्थिक पृष्ठभूमि के आधार पर ऑनलाइन समूह या फोरम से बाहर कर देना



किसी के अकाउंट का पासवर्ड चुराकर उस अकाउंट से किसी अन्य को उत्पीड़ित करने के लिए अवांछनीय/अनुचित संदेश भेजना

ऑनलाइन सुरक्षित कैसे रहें ?

क्या करें

- पासवर्ड गाइडलाइन के अनुसार मजबूत पासवर्ड का चयन करें, एवं उसके दुरुपयोग को रोकने के लिए उसको नियमित अंतराल पर बदलते रहें।
- सोशल नेटवर्किंग साइट के गोपनीयता सेटिंग्स को ध्यानपूर्वक पढ़ें।
- केवल अपने जानकार लोगों के साथ बातचीत करें।
- वेबसाइट पर बेहद सावधानी के साथ कोई भी फोटो/वीडियो या अन्य संवेदनशील सूचना पोस्ट करें क्योंकि उनके डिजिटल पद छाप हमेशा के लिए ऑनलाइन मौजूद रहते हैं।
- अगर आपको शक हो कि आपका अकाउंट हैक या चोरी किया गया है, तो तुरंत नेटवर्किंग साइट की सहयोग टीम को सूचित करें।
- यह सुनिश्चित करें कि कोई अधिकृत व्यक्ति ही कंप्यूटर सिस्टम या प्रयोगशाला तक पहुँचे।
- एक मजबूत नेटवर्क सुरक्षा तंत्र को सुनिश्चित करने हेतु निवेश करें।
- केवल प्रमाणिक ओपेन स्रोत या लाइसेंस युक्त सॉफ्टवेयर व ऑपरेटिंग सिस्टम का प्रयोग करें।
- अपने कंप्यूटर ऐसे व्यवस्थित करें कि वह स्वचालित एंटी-वाइरस सिस्टम एवं ऑपरेटिंग सिस्टम से जुड़ा रहे।

क्या न करें

- अपना पासवर्ड माता-पिता अथवा अभिभावक के अतिरिक्त किसी को न बताएं।
- किसी को भी अपनी व्यक्तिगत जानकारी जैसे कि आयु, पता, फोन नंबर, विद्यालय का नाम इत्यादि न दें क्योंकि इससे आपकी पहचान की चोरी का खतरा होता है।
- ऐसा कुछ प्रकाशित न करें जिससे दूसरों की भावनाएं आहत हों।
- अपने दोस्तों की जानकारीयां ऐसी नेटवर्किंग साइट्स पर साझा न करें, जोकि उन्हें खतरे में डाल सकती हैं।
- ऐसा कुछ भी आगे न भेजें जिसे आपने बिना किसी प्रमाणिक स्रोत के सोशल मीडिया पर पढ़ा हो।
- लॉग इन के बाद अपने अकाउंट को खाली न छोड़ें, यदि आप उपयोग न कर रहे हों तो लॉग आउट कर दें।
- किसी भी सोशल नेटवर्किंग साइट पर अपने लिए फर्जी प्रोफाइल न बनाएं।
- किसी भी सार्वजनिक नेटवर्क या कंप्यूटर पर अपने व्यक्तिगत उपकरण जैसे कि निजी यूएसबी अथवा हार्ड ड्राइव का प्रयोग न करें।
- सोशल नेटवर्किंग साइट्स पर किसी भी प्रकार के लिंक अथवा संलग्नक को न खोलें व .bat, .cmd, .exe, .pif जैसे फाइल विस्तार को सॉफ्टवेयर की मदद से ब्लॉक करें।

कानून आपकी मदद करता है!

साइबर उत्पीड़न सूचना एवं प्रौद्योगिकी अधिनियम, 2000 एवं भारतीय दंड संहिता के तहत दंडनीय अपराध हैं।

हर बच्चे और वयस्क को साइबर उत्पीड़न के मामलों की रिपोर्ट पुलिस को अवश्य दर्ज करानी चाहिए। (डायल करें: 112)



साइबर बुलिंग को कैसे रोकें व मुकाबला करें?



प्रतिक्रिया न दें

यदि कोई आपको परेशान कर रहा है तो उसी प्रकार की प्रतिक्रिया या प्रतिकार न करें। प्रतिक्रिया देना या प्रतिकार करना मामले को और बिगाड़ सकता है या आप मुश्किल में भी पड़ सकते हैं।



जितनी जानकारी इकट्ठा कर सकते हैं, करें

हर उस चीज़ का स्क्रीनशॉट लें जिसे आप समझते हैं कि ये साइबर बुलिंग हो सकती है और उसे सुरक्षित रखें।



ब्लॉक करें व सूचना दें

यदि कोई आपको परेशान करता है तो उसे ब्लॉक करें व सोशल मीडिया प्लेटफॉर्म पर अपराधी की सूचना दें। अधिकतर सोशल मीडिया प्लेटफॉर्म पर यह सुविधा उपलब्ध है।



इसके बारे में बताएं

भरोसेमंद वयस्क, जैसे कि अभिभावक व अध्यापक को बुलिंग की घटना के बारे में जानकारी दें। सहायता मांगें। अपने आप को कभी अकेला न समझें व इस बात को केवल खुद तक ही सीमित न रखें।



निजता रखें

अपनी सोशल मीडिया गोपनीयता सेटिंग्स को हमेशा उच्च स्तरीय रखें व ऐसे किसी भी व्यक्ति से न जुड़ें जिसे आप वास्तविक रूप से न जानते हों।



सचेत रहें

साइबर दुनिया में सुरक्षा व बचाव के उपायों के विषय में हमेशा नवीनतम जानकारी रखें।

सहयोग व हेल्पलाइन नंबरस

पुलिस: डायल करें **112** (पुलिस विभाग में साइबर अपराध शाखा होती है जो साइबर सुरक्षा के मामले को नियंत्रित करती है)

शिकायत दर्ज करें: **cp.ncpcr@nic.in**
(राष्ट्रीय बाल अधिकार संरक्षण आयोग)

चाइल्ड लाइन: **1098**

शिकायत दर्ज करें: **www.childlineindia.org**

शिकायत दर्ज करें: **cybercrime.gov.in**
(राष्ट्रीय साइबर क्राइम रिपोर्टिंग पोर्टल)
हेल्पलाइन नंबर पर संपर्क करें: **155260**
ट्विटर हैंडल: **@CYBERDOST**

शिकायत दर्ज करें: **complaint-mwcd@gov.in**
(महिला एवं बाल विकास मंत्रालय)