

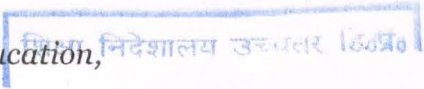
Most Urgent

No. EDN-H (21) A (1) PS-13/2017- Misc
Directorate of Higher Education
Himachal Pradesh

Dated: Shimla-171001 the October, 2017

To

All the Deputy Director of Higher Education,
Himachal Pradesh.



06 OCT 2017

Subject: - Regarding potential of information technology as a valuable learning resource is immense.

Memo,

Reference is invited to the Government letter No-EDN-B-Ga(17)-6/2016IX dated 22-09-2017 received from Principal Secretary (Education) to the Government of Himachal Pradesh (copy alongwith enclosures enclosed for your ready reference) and read this letter in continuation to this Directorate letter No. EDN-HE(21)B(15)15/2017-V-Vol-II dated 19th September, 2017, the instructions contained therein may be adhered to strictly in letter and spirit. Any laxity in this regard will be viewed serously.

Now again, in this regard, as per instructions contained in the D.O. No. 1-14/2017-RMSA dated 15th September, 2017 received from Joint Secretary (SE-1) to the Government of India, MHRD, Department of School Education & Literacy, Shastri Bhawan, New Delhi-110115 copy of which is already enclosed hereto as above, you are directed to issue the necessary detailed guidelines to every Government/Government aided and Private schools working under your jurisdiction in your District for safe and effective use of the internet in Schools and School Buses, so as to ensure the safety of every child in school.

Encls: As above. (03 pages)

-sd-

Director of Higher Education
Himachal Pradesh.

Endst. No. even Dated: Shimla-171001 the, October, 2017

Copy to:-

1. The Principal Secretary (Edu.) to the Government of Himachal Pradesh w.r.t. letter No. EDN-B-Ga(17)-6/2016IX dated 22-09-2017 for information please.
2. The Director of Elementary Education Shimla-1 for information and necessary action.
3. The Incharge, I.T. Cell, with the direction to upload the same on the Departmental website.
4. Guard file.

[Signature]

Director of Higher Education
Himachal Pradesh

D.No
1714685
21/9/17

No. EDN-B-Ga(17)-6/2016-IX
Government of Himachal Pradesh
Department of Higher Education

From

The Principal Secretary (Edu) to the
Government of Himachal Pradesh

To

✓
The Director, Higher Education,
Himachal Pradesh, Shimla-171001

Dated: Shimla-171002

22-9-2017

Subject:-

Regarding potential of information technology as a valuable
learning resource is immense.

Sir,

I am directed to enclose herewith a copy of Letter No. 1-14/2017-
RMSA-I dated 15th September, 2017 received from Joint Secretary (SE-1) to the
Government of India, MHRD, Department of School Education & Literacy, Shastri
Bhawan, New Delhi-110115, on the subject cited above and to request you to kindly take
further necessary action in the matter under intimation to this department.

Yours faithfully,

Joint Secretary (Edu) to the
Government of Himachal Pradesh

22 SEP 2017
Gen. Secy

54107754
21-09-2017

91



सत्यमेव जयते

Maneesh Garg,
Joint Secretary (SE-1)

Tel.- 011-23386232

Email: maneesh.garg@nic.in



सूचना का
अधिकार

भारत सरकार
मानव संसाधन विकास मंत्रालय
स्कूल शिक्षा और साक्षरता विभाग
शास्त्री भवन,

नई दिल्ली - 110 115

GOVERNMENT OF INDIA

MINISTRY OF HUMAN RESOURCE DEVELOPMENT
DEPARTMENT OF SCHOOL EDUCATION & LITERACY
SHASTRI BHAWAN,
NEW DELHI - 110 115

Do No. 1-14/2017-RMSA-I

Respected Ma'am/Sir,

15th September, 2017

As you are aware that, the potential of Information technology as a valuable learning resource is immense. However, if children use the internet without safety awareness, they may fall prey to illegal activity or abuse such as cyber bullying, fraud or something even more serious. Hence, awareness of internet safety norms is absolutely indispensable to make children free to explore knowledge without feeling intimidated. Increasing proliferation and sophistication of various electronic devices makes it all the more obligatory for schools to control and monitor their use by students.

2. Besides keeping an eye on the content student's access, parents and teachers should also be aware of what kids do and say online so that they do not compromise their privacy or safety. Over the past few years, social networking sites have become enormously popular among students. These sites can offer many benefits to their users, but some teens may not take sufficient care in protecting their privacy or may find themselves exposed to inappropriate content. Parents and educators can use Internet control software to block youths from accessing inappropriate content, but they should also be sure to educate themselves and their children or students about Internet safety.

3. In this regard, the detailed guidelines issued by CBSE for safe and effective use of internet in Schools and School Buses are enclosed herewith for your ready reference and for ensuring that similar guidelines are issued for all the Government & Government aided schools in your State/UT so as to ensure the safety of every child in school.

4. I would request that necessary action may kindly be taken at the earliest and this Ministry be apprised about the action taken.

With Regards,

Enclosure : As above

Yours sincerely,

(Maneesh Garg)

To,

Education Secretaries of All States/UTs.



20/9 ✓
JBE/...

S.O. (copy)

24/9
Anur

Subject: Guidelines for Safe and Effective Use of Internet and Digital Technologies in Schools and School Buses.

Schools need to promote a safe and secure educational environment for effective teaching and learning and to discourage students from actions detrimental to themselves, their peers and the value system. Schools are, thus, advised to take the following measures to pre-empt any inappropriate and illegal activity through IT enabled devices in schools:

- Educate students for the safe and effective use of the Internet.
- Make children explicitly aware of the rule for the acceptable use of the Internet and display rules in this regard prominently.
- Install effective firewalls, filtering and monitoring software mechanisms in all the computers and regularly review filtering and blocking policies and procedures. Various types of unsolicited contents available on internet must be blocked.
- Isolate Internet access from other school Network.
- Configure end user computer devices with parental control filters / Antivirus of appropriate standard.
- Deploy Digital Surveillance system.
- Make Children using the Internet to work in highly-visible areas of the school.
- Supervise and monitor all online activities in the light of educational objectives.
- Allow Children to access only pre-selected websites appropriate to their age group.
- Aware the teachers and other school staffs about Internet safety norms.
- Sensitise the parents about Internet safety norms.
- Take strict disciplinary action against those who attempt to bypass filtering or to access inappropriate or illegal material.
- Disable the usernames and passwords of those who leave the school promptly.
- Do not allow to create accounts for fictitious children or groups.
- Comply with all relevant legislation on copyright, property theft, fraud, discrimination and obscenity on all forms of IT enabled devices.
- Avoid digital and video images of individual students/teachers on school websites for safety of Children.
- Use only the licensed version of softwares.
- Draft a school policy on the safe use of electronic devices and implement it.

Safety of Children in the School Bus :-

2. It is advised that the mobile phone to be made available in each of the school bus to deal with unprecedented emergency should be of basic model without internet facility and data storage.
3. Schools are also directed to scrupulously follow the direction regarding restriction of using Mobile Phones in school environments and School Bus to ensure safety of children.
4. It is informed that carrying electronic communication devices including those that can store/record/play audio-visual content; transmit or receive images; or provide unfiltered connection to the Internet such as iPads, DVD/CD players, game consoles, handheld PC, smart phones, laptops, tablet or any other gadget with similar capabilities of data storage/transmission is not permitted in school and school bus without prior permission and verification of school authorities. The principal of the school and transport in-charge should check the mobile phone available with the attendant of the bus.
5. It is reiterated that unmonitored use of any electronic communication device is strictly prohibited in school and school bus and any reported violation in this regard would attract disciplinary action from the respective School.
6. Information Security Awareness materials for student, teachers, system administrators are available at <http://infosecawareness.in/>
7. Schools are directed to adhere closely to the above directions to preclude exploitation of children.