

NCERT issues guidelines on cyberbullying

‘Shield WiFi, Use Licensed Software’

New Delhi: Schools should consider contracting third-party vendors for cyber security, make sure the computers on campus have licensed software, and password-protect school Wi-Fi, said the National Council of Educational Research and Training (NCERT) in its guidelines for cyber safety. Issued in three parts, the guidelines are directed at schools, students and teachers. They outline dos and don'ts in addition to policy suggestions. This is the first time that NCERT has issued such a guideline.

Students are exhorted to “report online bullying immediately” to teachers, parents or someone they trust, to not bully others online “by teasing, threatening, using rude or offensive language, making derogatory or hateful comments, and to not “log in as someone else to read their emails or mess with their online profiles,” among other things. The guidelines issued on Tuesday also ask teachers to “regularly review browsing history on the devices being used by children” and “monitor device usage by students” and not to engage with cyberbullies.

This February, a cyberbullying incident from a Gurugram school where a

“ These guidelines can provide a framework for our own policies. If there is some kind of cyberbullying, we should also involve the parents as they often don't get to know

TANIA JOSHI
Principal, The Indian School

Class VIII student threatened to rape a teacher and harm her daughter in an Instagram post had caused much concern among parents and schools, prompting a rethink of policies dealing with such behaviour.

“These guidelines can provide a framework for our own policies,” says Tania Joshi, principal, The Indian School, New Delhi. “We already have an anti-bullying committee which is mentioned in the school almanac. If there is some kind of cyberbullying, we should also involve the parents, because they often don't get to know,” she says.

Students too have welcomed the move. Besides standard recommendations relevant to their roles, the guidelines also spell out general safety measures that are usually prescribed for all internet users. These include logging out of online sessions when not in use, not saving passwords, guarding against phishing scams, avoiding clicking on suspicious links, and not downloading email attachments from dubious sources.