Supporting CIPA requirements in US School Districts

In 2000, Congress passed the Children's Internet Protection Act (CIPA) to help combat the growing concern of children accessing obscene or harmful content on the Internet.

Any K-12 school or library that accepts certain federal funds is required to use a "technology protection measure" on every computer connected to the Internet to block or filter any harmful content.

CIPA requirements include the implementation of an Internet safety policy addressing:

- Access by minors to inappropriate matter on the Internet;
- The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;
- Unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information regarding minors;
- Measures restricting minors' access to materials harmful to them.

Schools and libraries who cannot certify that they have an Internet safety policy (including technology protection measures) may not qualify to receive their federal fund.

How does NetSupport DNA support CIPA?

IT Asset Management solution, NetSupport DNA, includes a built-in Internet safety module containing both proactive and reactive tools that are relevant, effective, and, most importantly, up to date.

> "The eSafety features are great in providing alerts when students are interacting with potentially harmful materials online."
>
> - Hillcrest Academy

Working with the Internet Watch Foundation, partners and schools, NetSupport DNA contains a sophisticated **keyword and phrase monitoring tool** which also includes multiple **language packs**, allowing schools to gain an insight into what students are typing, searching for or copying online – regardless of language.

An innovative **word cloud** highlights trending topics across the school to help put incidents into a broader context, while appropriate staff can be alerted through email, real-time pop-ups or summary reports, prompting them to **review the triggered event**.

The **Contextual intelligence-based Risk Index** automatically flags high-risk events and vulnerable students and creates a risk index number for each event, based on sophisticated contextual intelligence risk analysis.

Vulnerable students can be flagged and tracked for extra support, and a **'history of concerns'** is available for each one. Teachers can also add any concerns they have about a student. In addition, students' internet activity can be tracked and managed (incl **age appropriate filters**) via the **internet monitoring tools**, while **application metering** reports reveal application use; helping to ensure usage complies with school policy.

The **cloud-based online safety console** also allows staff to access key information and alerts from triggers across the school's local network while on the go.

Internet safety needs to be proactive too, so NetSupport DNA enables students to access **online support resources** – covering topics such as FGM, drug addiction, grooming and bullying – all from the NetSupport DNA internet safety icon on their PC. Students can also report their concerns in confidence to a trusted member of staff via the **Report a Concern** option.

> "Trying to list all the websites that students shouldn't be accessing is 'like counting stars in the heavens'. The more I use the software, the more I appreciate its functionality."
>
> - Summit Preparatory School Montana