14.7% of students in Texas were cyberbullied 12 months before the survey.
CDC state YRBS data 2017

Supporting David's Law - 85th Texas Legislative Session

David's Law aims to bring awareness and enforce new policies related to cyberbullying prevention and mediation to schools.

What is cyberbullying?

As defined by David's Law, "Cyberbullying" means "bullying arising from a pattern of acts or one significant act that is done through the use of any electronic communication device, including a cellular or other type of telephone, a computer, a camera, electronic mail, instant messaging, text messaging, a social media application, an Internet website, or any other Internet-based communication tool."

How are schools affected by this law?

✓ This law applies to public schools, as well as open-enrolment charter schools. Private schools are not included.

✓ Schools must have a notice procedure in place under their bullying policy.

✓ Schools must notify the parent or guardian of the alleged victim by the third business day after an incident is reported.

✓ Schools must notify the parent or guardian of the alleged bully within a reasonable amount of time after the incident is reported.

✓ Schools must have procedures in place to allow students to report an incident anonymously.

✓ A principal or a person designated by the principal (other than a school counselor) can report bullying that rises to the level of being a crime to law enforcement officials.

✓ Schools can remove a student who is engaging in bullying activity from class and place them in a disciplinary alternative education program or expel them, if they encourage a student to commit or attempt to commit suicide.

✓ Schools and school personnel who report criminal bullying to law enforcement gain strong protection from civil or criminal liabilities and from disciplinary action.

✓ A school counselor's responsibilities will now include acting as an impartial, non-reporting resource for interpersonal student conflicts concerning bullying.

✓ Schools must promote mental health education.

✓ Cyberbullied minors (or their parent/guardian) can now seek injunctive relief (such as a temporary restraining order and/or an injunction) against the cyberbully and their parents.

In this document, we outline how our Classroom Management solution (NetSupport School) and our IT Management and Internet Safety solution (NetSupport DNA) can offer support to students in need – and help schools meet their requirements in line with this law.

NetSupport School

In a classroom, teachers using NetSupport School can set **authorized/restricted website and application lists**, as well as completely block Internet access. These types of settings can be used as a default mode for lesson start-up, removing the need for the teacher to apply settings before the students have a chance to explore online.

Teachers can also **monitor students' current Internet use** by viewing real-time thumbnails of their PCs. A record of Internet history use is also created and can be printed or saved for future reference.

Real-time keyboard monitoring provides a simple view, listing each active student and their current keyboard input (excluding password fields).

NetSupport School also helps teachers educate about positive digital interactions and how to behave responsibly online in a safe learning environment. Teachers, for example, can **show their screen or a student's screen** to the rest of the class to promote positive use.

NetSupport DNA

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

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.

> " **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 "

The **Contextual intelligence-based Risk Index** automatically flags high-risk events and vulnerable students, creating 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. Students can also **report a concern** in confidence to a teacher they trust, and Teachers can also add any concerns they have about a student.

In addition, students' Internet activity can be tracked and managed via the **Internet monitoring tools**. With the creation of profiles, schools can meet the need of each year group – ensuring that Internet access is age-appropriate while allowing the students the flexibility to learn about the online world.

Apps and games can also be blocked or restricted by their window's title, helping schools to add an extra layer of security while keeping students on task. Meanwhile, **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.

These products are available in: