bark

Monitoring accounts for school safety: AI, data, and technology

Introduction to Bark for Schools

Students growing up in the 21st century have witnessed the rise of incredible digital technologies. This progress has changed the way students navigate the world, both in positive and negative ways.

On the one hand, they're able to collaborate on projects and access more information than ever before. But they're also better equipped to abuse digital technologies — as well as fall victim to abuse. **In 2025, Bark analyzed billions of digital interactions across its monitoring platforms, revealing persistent and growing risks to student safety in areas such as self-harm, bullying, violence, and substance-related content.**

Digital technologies have also accelerated the rate at which language evolves, as their development compels corresponding developments in speech and writing. Artificial intelligence and machine-learning techniques provide a way for us to keep pace with these developments, which is especially important when it comes to protecting students from the worst of what exists online. Bark — and the Bark for Schools initiative — is pioneering natural language processing systems to help keep kids and students safe in the digital age.

Bark for Schools monitors millions of online activities each day. This work involves sensitive student information, and we believe student safety should never come at the cost of student privacy.

How we protect student data

- ✓ Schools and districts own all user data
- ✓ Schools control what is monitored
- ✓ Data is encrypted in storage and in transit
- ✓ Student activity data is automatically deleted after 15 days
- ✓ We never sell student data
- ✓ We do not share data with third parties without consent

We are committed to transparency in our data collection and analysis practices. The following document provides a comprehensive overview of how Bark for Schools monitors, protects, and supports student safety.

What is Bark?

Founded in 2015 by a dad of two, Bark is an online safety company that helps families protect their kids online and in real life. Over the past decade, we've transformed into the industry leader of safer tech for children, garnering recognition from TIME, Wired, The New York Times, Forbes, and countless other publications.

We're at the forefront of the online safety revolution, designing and building smart devices that families need with parental controls that actually work. Our Bark Phone, Bark Watch, Bark Home, and Bark app are enabling today's parents to help keep their kids safe like never before — and we're just getting started.

Bark is also deeply committed to education and community impact. Through our Bark Community Partners program, we work with schools, nonprofits, and local organizations to provide online safety resources, training, tools, and safer technology to families and educators.

Bark for Schools

Bark's flagship product helps parents monitor and manage their children's personal accounts and devices. But in 2018, after the tragic Parkland shooting, we realized that we had the resources to provide the same service — in addition to others — to schools, and to do so in a way that keeps them from spending thousands of dollars each year to protect their students from the worst dangers of the online world.

We developed Bark for Schools to give back to our communities and to help keep children safe — by providing core monitoring at no cost to eligible K–12 schools, with optional paid enhancements available through Bark for Schools+.

One of the fastest-growing companies in EdTech, we now help protect more than 3,700 school districts and approximately 6 million students across the country — with dozens more joining every month.

> “We developed Bark for Schools because we strongly believe cost shouldn’t be a barrier to student safety.”

What Bark for Schools monitors

Bark for Schools offers monitoring of school-issued Google Workspace and Microsoft 365 accounts, with specialized extensions available for Chrome, Chromebook, and Microsoft Edge. Monitoring capabilities vary by product tier.

Google Workspace

Gmail: Subject, body, attachments (images and videos)

Gmail: Inline images (Bark for Schools+)

Google Drive: Images, videos, Office documents (.doc, .docx, etc.), plain text files

Google Docs: Document title, text within the document, comments, and replies

Google Docs: Inline images (Bark for Schools+)

Google Slides: Presentation title, text and emojis on slides, comments, and replies (Bark for Schools+)

Google Sheets: Spreadsheet title, text within cells, comments, and replies (Bark for Schools+)

Google Chat: Text and attachments (images, videos) in direct messages*

Google Chrome: Webpage titles and searches**

** Ensure Google Chat settings are configured correctly.*
*** Requires deployment of the Bark for Chrome extension via Google Workspace.*

Microsoft 365

Outlook: Subject, body, attachments (images and videos)

Outlook: Inline images (Bark for Schools+)

Teams: Text, images, and videos in direct messages

OneDrive: Images, videos, Office documents (.doc, .docx, etc.), plain text files

Word Docs: Content, comments, and replies

Word Docs: Inline images (Bark for Schools+)

Microsoft Edge: Webpage titles and searches*

** Requires deployment of the Bark for Edge extension via Microsoft 365.*

Parent Portal

Students still use their school-issued accounts after classes have let out, and during those times there may not be a reviewer available to respond to urgent alerts. The Parent Portal allows schools to enlist the support of parents and guardians to receive alerts about their children after hours and during breaks. Enabling the Parent Portal is a positive step toward more comprehensive monitoring to help keep students safe online.

Integration options

Bark for Schools supports multiple integration options to help districts efficiently manage Parent Portal contact information and reduce manual administrative work. These integrations allow schools to securely sync required contact details — including student and parent/guardian email addresses — directly into Bark for Schools for use with Parent Portal invitations and alert delivery.

Parent Portal contacts can also be uploaded using a .CSV file directly within the Bark for Schools dashboard. From the Parent Portal settings page, schools can select their preferred contact sync method. This function is available for any school using Bark.

Once enabled, Bark sends unique Parent Portal activation links to each parent or guardian on behalf of the school.

Clever

Clever and Bark

Schools and districts using Bark for Schools+ and Clever can securely sync student and parent/guardian email addresses for the Parent Portal through their existing Clever environment. This integration simplifies setup by reducing the need for manual data entry and allowing administrators to leverage existing roster data.

ClassLink

ClassLink and Bark

Bark for Schools also integrates with ClassLink, allowing districts to manage Parent Portal invitations through their existing ClassLink environment. Using ClassLink's roster and permissions framework, schools can securely share student and parent/guardian email addresses with Bark for Schools for the purpose of Parent Portal activation.

Data and technology overview

Data control and ownership

Schools and school districts are the absolute owners of all student data, and they also control the level of monitoring. Bark understands that there is no one-size-fits-all solution for school safety, and allowing each school to serve as the owner and controller of data and monitoring frees them to determine what's most appropriate for their particular institution.

We have implemented a number of features that make the Bark for Schools platform extremely easy to set up and use while maintaining a high standard of protection.

Security and compliance overview

Security is one of Bark's highest priorities. Bark for Schools adheres to the requirements of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy of student education records. In addition to federal requirements, many states have adopted their own student privacy legislation, and Bark is designed to meet or exceed applicable state and federal standards.

Bark maintains a SOC 2 Type II compliant security program, reflecting our commitment to strong internal controls around data security, availability, and confidentiality. These controls are independently audited and help ensure that student data is protected throughout its lifecycle.

Bark for Schools is also designed to support schools in meeting their obligations under laws such as the Children's Internet Protection Act (CIPA) and the Children's Online Privacy Protection Act (COPPA), while allowing districts to retain control over monitoring configurations, data access, and local policy decisions.

Our technology

Context is extremely important to properly classify a conversation. Without context, computers are unable to determine whether a specific chat message is a joke, song lyrics, sarcasm, or something more serious. As the way students communicate continues to evolve, traditional keyword-based detection methods often fall short.

Modern machine-learning developments have allowed Bark to analyze language contextually, improving our ability to determine whether a piece of text represents a potential safety concern. Bark's technology is specifically designed to understand childspeak — the slang, abbreviations, emojis, humor, and evolving language patterns commonly used by children and teens in digital environments.

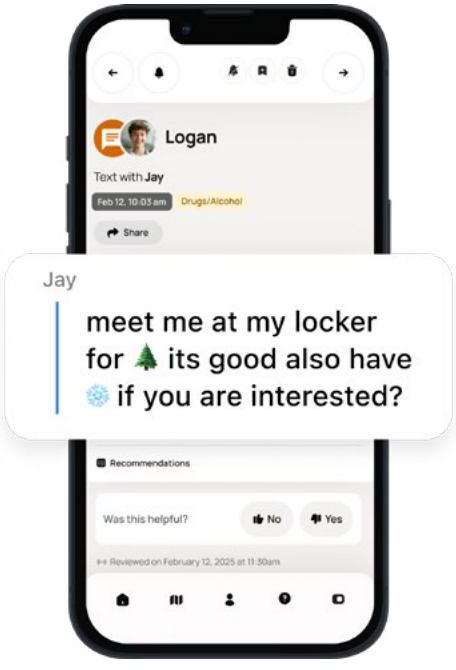
Our underlying detection systems analyze language in relation to surrounding conversation, historical patterns, and behavioral signals, rather than relying on isolated words or phrases alone. This contextual approach helps distinguish between benign conversations and situations that may indicate real risk, reducing false positives while ensuring concerning content is surfaced appropriately.

Bark also uses a multi-label approach, which allows signals associated with one category of concern to inform detection across others. For example, language related to bullying, depression, or self-harm may overlap, and analyzing these signals together provides a more accurate understanding of intent and severity. This approach, informed by large-scale, real-world data, allows Bark's detection capabilities to continuously adapt as student language and behavior change over time.

We've heavily invested in a robust Data Annotation team in the U.S. that gives us the capacity to properly label tens of thousands of pieces of data each day flagged by our algorithms. This labeled data is then fed back into a data ingestion process that trains the algorithms nightly. Our investment in this process has given us the ability to stay current with the variations in language, as well as the flexibility to adapt on the fly as we encounter new topics and phrasings among student conversations.

Bark picks up on the details

The way students communicate online changes constantly. Bark's contextual analysis allows the platform to identify potentially harmful or inappropriate language even when it appears in emojis, slang, acronyms, or indirect phrasing. By focusing on how language is used — not just the words themselves — Bark is better equipped to surface meaningful safety signals while minimizing unnecessary alerts.



Detection and data annotation

It's important to note that no monitoring service can promise complete and total detection of online issues. Adapting to the evolution of language is a perpetual challenge, and monitoring services are often limited by the closed nature of the platforms they are charged with monitoring. Snapchat and Instagram, for example, do not offer APIs that are conducive to third-party integration, which makes it difficult for monitors to detect every potential issue.

Furthermore, Bark allows schools and districts to exercise broad authority over which activities are monitored, as well as how sensitive our detection algorithms are to potential alerts. Schools should be advised that adjusting the sensitivity levels has an effect on accuracy. Higher sensitivity may produce false positives, and lower sensitivity may produce false negatives.

That said, the years we've invested in refining our technology have produced an algorithm with a high rate of accuracy. In addition to the wealth of data collected for contextual analysis, this is in large part due to our dedicated Data Annotation team.

Review and escalation

The Data Annotation team consists of specialists trained to review and validate high-severity alerts identified by Bark's detection systems. All team members undergo background screening appropriate to the sensitive nature of this work and are trained to interpret contemporary student language, including slang, abbreviations, and evolving digital communication patterns. By confirming or dismissing alerts, the team supports ongoing refinement of Bark's detection models.

Reviewers primarily encounter anonymized student data. In limited cases involving severe escalation, designated review team leaders may access additional contextual information necessary to evaluate potential risk. This layered review process helps ensure that high-severity alerts are assessed thoughtfully and responsibly.

Bark works with law enforcement at the federal, state, and local levels and may escalate cases involving potential grooming, exploitation, drug trafficking, or credible threats of imminent harm to the appropriate authorities. Bark also works with the National Center for Missing and Exploited Children (NCMEC) in cases involving suspected sexual exploitation, consistent with applicable reporting obligations.

When a high-severity alert is identified, Bark for Schools applies an escalation process designed to support timely district awareness and response.

For Bark for Schools+ customers, designated reviewers may receive enhanced, multi-channel notifications — which can include phone outreach, text message alerts, and email — when an alert is determined to require urgent attention.

For districts using the core Bark for Schools monitoring service, severe alerts are delivered via email notification within the Bark for Schools platform.

Notification methods and escalation workflows may vary based on district configuration and service tier.

We recommend that districts designate appropriate personnel to receive and manage high-severity alerts and maintain up-to-date contact information within the platform. Critically severe alerts — such as those involving credible threats of violence — may require prompt district review. Because student activity can occur outside regular school hours, districts may choose to enable Parent Portal to extend alert visibility to families during evenings, weekends, or school breaks.

Severity and type

Activities that Bark's algorithms label as abusive are categorized by "Severity" and "Type." These two measures are weighted so they can be scored on the same scale. If the aggregated severity level is high enough, then it will be automatically escalated to the Data Annotation team. Alerts are also given a Confidence Score, which is the computer's level of certainty that the alert is legitimate. If the Confidence Score is high enough, the alert will be auto-sent, notifying reviewers directly through the Bark for Schools platform.

Severity is a measure of the seriousness of a potential issue, as judged by our technology's contextual analysis — the higher the number, the more severe the alert. For example, a student sharing plans to bring a gun to school is more severe than a student wishing a classmate would die.

Type describes what kind of issue has been detected, like "Bullying" or "Suicide / self-harm." Each type of abuse has a different threshold for escalation, and between the provided examples, suicidal ideation would be rated higher than an instance of bullying. Check out our Escalation Process guide for more information.

Abuse Types include:

- Bullying
- Sexual content
- Depression
- Self-harm or suicidal content
- Drug/alcohol related content
- Violence
- Hate speech
- Sextortion
- Other (including profanity, predatory behavior, dangerous organizations, weapons, etc.)

Reports and analytics

Schools and districts have self-service access to reporting and analytics within the Bark for Schools dashboard, providing visibility into behavioral trends based on student activity monitored since installation. Reports can be filtered by time range, alert category, platform, and organizational structure (such as organizational unit, group, or grade level), allowing administrators to quickly identify patterns and investigate incidents.

For example, if a serious incident occurs on campus, administrators can review historical data related to bullying to understand frequency, timing, and platforms involved, and cross-reference related behaviors such as depression or hate speech to inform an appropriate response.

In addition to dashboard analytics, Bark's Customer Success team may provide Insight Reports to Bark for Schools+ customers during scheduled success reviews or upon request. These reports offer a deeper, aggregated view of behavioral trends across monitored groups, along with representative examples of high-severity alerts during the reporting period. Insight Reports are designed to support district stakeholders in identifying patterns, evaluating policy effectiveness, and informing ongoing safety planning.

Schools and districts retain full ownership of all student data. Bark for Schools monitors and analyzes that data on their behalf to help support student safety.

Chrome and Chromebook

Our monitoring service provides a specialized browser extension for Google Chrome, which is the inherent browser on Chromebooks. As Chromebooks are among the most popular devices issued to students in 1:1 districts, this extension allows Bark for Schools to monitor browser activity with the same proficiency as with the broader Google Workspace account.

The benefits of a built-in monitoring extension for Chrome are significant. While students can log out of Google Workspace or Microsoft 365 accounts, managed Chromebook environments help reduce opportunities for students to bypass monitoring, since the browser is native to the device and centrally administered.

Other functionalities include:

- Account-level monitoring
- URLs
- Page titles
- Web searches
- Parent Portal

Storage and security

Secure databases

All data that is monitored by Bark for Schools is stored in an encrypted database. Some companies keep this kind of data stored in plain text, and when they're hacked, it is easy to read and exploit that data. Bark for Schools has precluded this possibility, so a hacker would be unable to decrypt information stored in our database.

Web browser sessions

Web browser sessions are also encrypted and authenticated with SSL, meaning that all information moving between the web servers and browsers is kept completely private. No one can infiltrate these transfers without a unique cryptographic key issued by a Certificate Authority. Our certificate is issued by DigiCert, Inc., which uses the SHA-2 hashing algorithm to make it impossible for someone to modify or fake our certificate. Any such attempt triggers an error and prevents the attacker from making a secure connection.

Backups and data removal

The Bark for Schools databases are backed up every night and retained for a full week. They are also tested weekly to ensure that they can be restored. After seven days, the backups are purged entirely.

Data related to student activities is not included in the weekly purges, however. As noted previously, context is an essential component of our monitoring services. Our technology — as well as our team of human reviewers — requires a more protracted analysis in order to detect issues that develop over time. Accordingly, student activities are stored for 15 days and then purged as part of Bark for Schools' standard data retention practices.

Amazon Web Services

Amazon Web Services (AWS) is a known and trusted partner in the cybersecurity industry, and they handle all of our database encryption needs. By working with such a reliable service provider, we are able to focus our efforts on Data Annotation, business development, and other necessary aspects of helping to keep children safe online.

State and federal compliance

Privacy and data security are at the top of people's minds when it comes to online activity. In light of hacks and data breaches of increasing severity, individuals and organizations alike want to ensure that they are protecting both themselves and those who depend on them.

Signing up for Bark for Schools helps keep students safe online, and the data we collect is secured using state-of-the-art technologies and best practices. Bark for Schools is designed to support schools in meeting applicable state and federal compliance requirements.

Children's Internet Protection Act (CIPA)

Protects minors from obscene or otherwise harmful online content at school.

Requires adoption of an internet safety policy that:

- Blocks or filters inappropriate content
- Monitors students' online activities
- Provides education about appropriate online behavior

How Bark for Schools can help

Bark for Schools provides free monitoring services for K–12 accounts, including email, documents, and cloud storage solutions offered by Google Workspace and Microsoft 365. Bark also supports web filtering through domain-level controls to help schools meet CIPA-related requirements, including those tied to E-rate funding.

Children's Online Privacy Protection Act (COPPA)

Prohibits deceptive online practices related to the collection, use, or disclosure of personal information of children under the age of 13. COPPA requires transparency around data use, confidentiality, and retention practices.

How Bark for Schools can help

Bark for Schools is designed for use in school-based environments, where districts act as the consenting authority for student data use. Bark aligns with applicable COPPA requirements through contractual agreements, privacy controls, and data minimization practices. Student activity data is retained for a limited period consistent with Bark for Schools' standard data retention policies.

Federal Educational Rights and Privacy Act (FERPA)

Provides rights to parents and eligible students regarding education records, including the right to review and request correction of those records. Schools must generally obtain written consent before disclosing information from a student's education record.

How Bark for Schools can help

Bark for Schools does not disclose student information to third parties without prior written consent unless required by law or pursuant to a court or administrative order. Bark for Schools operates as a "school official" with a legitimate educational interest under FERPA and may process data on behalf of schools to help protect the student body.

California Assembly Bill No. 1584

Authorizes educational agencies to contract with third-party providers under specific requirements. Applies to providers of electronic services for:

- Digital storage, management, and retrieval of student records
- Educational software that allows third parties to access, store, and use student records

How Bark for Schools Can Help

Bark for Schools supports schools and districts in meeting the requirements of California Assembly Bill No. 1584 by operating as a service provider to educational agencies and handling student data solely on their behalf. Bark for Schools' data practices are governed by contractual agreements and align with applicable federal and state student privacy laws, including FERPA, as well as industry-standard student data privacy commitments.