bark
FOR SCHOOLS

The Administrator's Guide to Bark for Schools

What is Bark for Schools?

Bark for Schools is on a mission to make sure that no school goes without the tools they need to help keep their students safe online and on their devices. Schools are often under tight budgetary constraints, but that shouldn't prevent them from accessing the safety resources they need. Bark for Schools offers free web filtering as well as monitoring of school-issued Google Workspace and Microsoft 365 accounts, with specialized extensions for Chrome and Chromebook, to all public and private K-12 schools in the United States.

One of the fastest-growing companies in EdTech, we now help protect more than 3,000 school districts across the country — with dozens more joining every month.

In 2021, Bark for Schools detected millions of concerning situations on school-issued accounts, including:

- **388,270** instances of children buying, selling, or discussing illicit drugs
- **110,276** students involved in bullying
- **67,535** children expressing self-harm, cutting, and/or suicidal thoughts

School-focused Corporate Responsibility

We offer Bark for Schools at no cost as a way to give back to our communities and to help keep children safe. 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.

> "The best thing we can do to keep people safe is to intervene as quickly as possible."
>
> —Mike Kuhlman
>
> Superintendent, Hart District

The History of Bark

Bark for Families is an award-winning service that monitors text messages, email, YouTube, and 30+ apps and platforms for potential safety concerns like online predators, adult content, bullying, drug use, depression, suicidal thoughts, and more. We also offer screen time management and web filtering to empower families to help protect their children's entire online worlds.

Created in collaboration with child psychologists, youth advisors, digital media experts, and law enforcement professionals, Bark delivers a research-backed solution for helping safeguard children as technology changes how and where we communicate.

What's a neural network?

A neural network is a network architecture with node layers inspired by how neurons in a human brain work. Neural networks are incredibly useful with sequential data because each neuron or unit can use its internal memory to maintain information about the previous input. With human generated language, "I had my homework stolen" is much different than "I had stolen homework." This allows the network to gain a deeper understanding of the statement.

The Nuts and Bolts: Content Monitoring Powered by A.I.

Context is extremely important to properly classify a conversation. Without context, computers are unable to determine whether a specific chat message is a joke or something more serious. Through the development of modern machine-learning techniques, we've been able to analyze that context and make better decisions about whether a piece of text is a potential alert.

Our underlying network is based on a neural network trained on custom word embeddings to aid in understanding the variations of childspeak. We also use a multi-label approach, which allows us to use the triggers from one abuse type towards another. The combination of this approach trained on billions of data points has allowed us to create a perpetually improving natural language processing (NLP) system.

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 data points each day. This labeled data is then fed back into a data ingestion process that trains the algorithms nightly. Our investment in this process has allowed us to stay current with the variations in language, and it gives us the flexibility to adapt on the fly as we encounter new topics and phrasing among student conversations.

Parent Portal

Students still use their school-issued accounts after classes have let out, and during those times there may not be an administrator 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 towards more comprehensive monitoring to help keep students safe online.

Clever and Bark

Schools can use Clever to sync family contact information by downloading the Bark for Schools app. This feature greatly simplifies the Parent Portal setup, removing the need to manually input data and allowing administration to spend their time on more important things. Schools can also launch Parent Portal by uploading a .CSV file to their Bark for Schools dashboard.

What We Monitor

Google Workspace

- **Gmail**: Subject, Body, Attachments (Images and Videos)
- **Google Chat:** Text and Attachments (Images and Videos) in Direct Messages
- **G Drive**: Photos, Videos, Office documents (.doc, .docx, etc.), Plain Text Files
- **Google Docs**: Content, Comments, and Replies

Microsoft 365

- **Outlook**: Subject, Body, Attachments (Images and Videos)
- **OneDrive**: Photos, Videos, Office documents (.doc, .docx, etc.), Plain Text Files
- **Teams**: Text, Images, and Videos in Direct Messages

Google Workspace and Microsoft 365 are extremely popular in schools, with many children using both for schoolwork, homework assignments, and even group projects. But kids are incredibly inventive, and they've managed to turn platforms like Google Docs into a de facto communication platform — whether with other students or as personal diaries — necessitating monitoring.

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 these browsers and devices with the same proficiency as with the broader Google Workspace account.

The benefits of a built-in monitoring extension for Chrome cannot be understated. While students can log out of Google Workspace or Microsoft 365 accounts, Chromebook users are generally unable to circumvent our monitoring service because the browser is native to the device.

As well as being fully Parent Portal-enabled, other functionalities include account-level monitoring, URLs, page titles, and web searches.

Web Filtering

Internet access is a critical component of modern K-12 curricula, and Bark's web filtering feature allows schools to create and enforce an acceptable access policy that is tailored to the needs of their school. Our web filter allows for the whitelisting and blacklisting of any site, and offers the function to disable access to certain sites of a given category, including adult content, illegal content, streaming services, social networking/chat sites, and more.

Built and designed with feedback from schools across the country, this feature is fully customizable, requires no hardware, and is controlled from a single interface within the Bark for Schools dashboard. Alongside this, we also provide details for site visits on a student level, empowering administrators to make informed decisions on student web traffic behavior.

> "Our free service can be up and running within minutes"

DNS Web Filter

We offer a DNS filter for an on-site, network-wide solution, which allows you to:

- Whitelist/blacklist specific websites
- Whitelist/blacklist entire web categories
- Reporting on general network traffic
- Display top visited sites
- Display top blocked sites
- Display requests-by-day chart
- Reporting on IP-specific traffic
- **Can be deployed on-site**
- **Great for filtering all devices connected to the school network**

Chrome Web Filter

We offer a Chrome extension web filter that enforces policies wherever the student is logged in to their school account so you can:

- Whitelist/blacklist specific websites
- Whitelist/blacklist entire web categories
- Reporting on Organizational Units
- Reporting on individual students
- Display top visited sites
- Display top blocked sites
- Display requests-by-day chart
- Account-level monitoring
- **Can be deployed remotely**
- **Great for Chromebooks**

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.

> "Our algorithm can detect harmful or inappropriate language even if it's only in emojis, slang, or acronyms."

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 30 days, but at the request of a school or district, they may be removed in 15 days.

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.

Monitoring Content Categories

Severity and Type

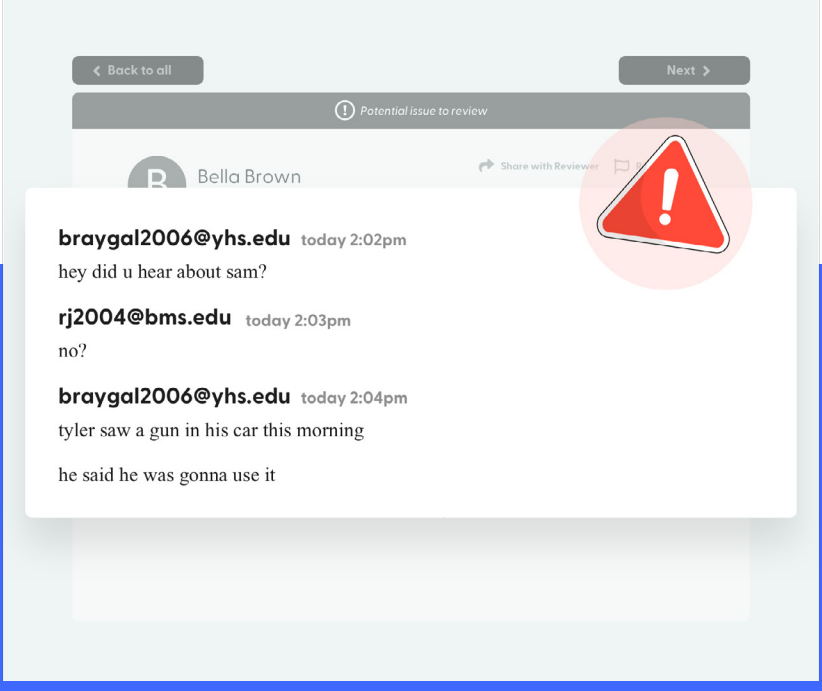
Activities that Bark's algorithms label as Abusive are categorized by "Severity" and "Type." These two measures are weighted so they can be scored on the same scale. If the aggregated severity level is high enough then it will be automatically escalated to the Data Annotation team. Alerts are also given 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.)



Abuse Types

Bullying

Communications that indicate bullying range from less severe instances of teasing and unfriendly joking all the way to explicit threats of violence and encouraging self-harm.

Sexual Content

Sexual content may include less severe examples such as emails from Victoria's Secret all the way up to explicit images and/or messages (sexting).

Depression

Examples of depression range from messages revealing low confidence to extremely concerning issues questioning self-worth and suggesting an inability to cope.

Self-harm or Suicidal Content

With these messages, the algorithm catches even joking references to suicide (e.g., "this homework makes me wanna die") as well as serious, life-threatening messages from kids that indicate a wish to take their own lives.

Violence

These range from milder examples quoted from film and television all the way to threats in which a student expresses imminent plans of violence.

Hate Speech

Bark defines hate speech as a message that is derogatory or aggressive towards people based on their race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, or serious disabilities or diseases. Hate speech examples range from obvious, tasteless jokes to violent threats.

Predatory Behavior

Predatory behavior is used by child predators to establish trust with children in order to persuade them into engaging in risky behavior. Bark is able to monitor and alert school administrators to these communications by identifying coercive language and speech patterns used by adults, even when those adults are pretending to be children.

Other abuse types

- Profanity
- Drug/Alcohol Related Content
- Sextortion
- Dangerous Organizations
- Weapons

Human Escalation and Review

The Data Annotation team consists of specialists trained to review and confirm instances of abuse that our algorithms detect. They are spread all across the U.S. so that they can be responsive to alerts around the clock, regardless of the time zone, and they are all well-versed in the nuances of contemporary American slang. By confirming or overruling alerts to abuse, the team contributes to the daily improvement of our algorithms.

Reviewers on the Data Annotation team only encounter anonymized student data, and only in the event of a severe escalation are the review team leaders able to see more specific information. By studying communications at the human level, they are able to make more informed decisions and ultimately coordinate the appropriate response to prevent a tragedy from unfolding.

Bark works with law enforcement at the federal, state, and local levels, and our team escalates cases of potential grooming, exploitation, drug trafficking, or imminent risk to a student's life to the appropriate authorities. We also work with the National Center for Missing and Exploited Children (NCMEC) in cases involving sexual exploitation.

In escalated situations, email alerts are triggered to notify relevant parties so they can stay apprised of the situation and the individuals involved. After issuing a severe alert, we track the alert for 24 hours. If schools don't review the alert within that time, the Data Annotation team leaders send emails after judging that the alert is serious enough to merit the school's immediate involvement.

We highly recommend that schools have a designated team to field alerts from Bark. We also recommend that schools have at least two contacts, as well as a mobile phone number listed for immediate communications with Bark. Severe alerts — like a school shooting threat — are often time sensitive, so it's imperative that a contact is available. Alerts may also occur after school hours and during holidays, when many students are still using their school-issued accounts. Schools can allow parents to receive alerts during these times by enabling the Parent Portal.

> "We highly recommend that schools have a designated team to field alerts from Bark."

State and Federal Compliance

Privacy and data security are at the top of people's minds when it comes to their online activities. 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 with state-of-the-art technologies and best practices. Bark for Schools can also help schools meet certain state and federal compliance regulations.

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 all K-12 accounts, including email, documents, and cloud storage solutions offered by Google Workspace and Office 365. We also filter web domains at the student account and DNS levels.

Children's Online Privacy Protection Act (COPPA)

Prohibits deceptive online practices for the collection, use, or disclosure of personal information of children under 13. Site operators must provide parental notice and consent, review processes, confidentiality, data retention and deletion statements, and more.

How Bark for Schools Can Help

Bark for Schools does not collect data from children under 13 without parental consent. Data is also automatically deleted after 30 days, and upon request, user data may be deleted within 15 days.

Federal Educational Rights and Privacy Act (FERPA)

Provides rights to parents and eligible students over education records, including the right to review and correct the student's records. Schools must generally have written consent to release information from a student's record.

How Bark for Schools Can Help

Bark for Schools does not disclose information to any third party without prior written consent unless pursuant to court or administrative order. Bark for Schools is also considered a "School Official" with legitimate educational interest under FERPA and may share without consent to 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 is an at-will service provider and is therefore not subject to third-party contract requirements. But because Bark for Schools complies with COPPA and FERPA, it also satisfies several tenets of AB 1584.

Bark for Schools Privacy and Security Checklist

- ✅ Schools and districts own all user data
- ✅ Schools control the level and degree of monitoring
- ✅ Data stored in encrypted database
- ✅ Web browser sessions use SSL encryption
- ✅ Data purged within 30 days of analysis
- ✅ No data sold or given to third parties without consent
- ✅ Consent may be withdrawn at any time

> "Bark for Schools is the real deal. We didn't have any sort of content scanning before getting Bark. When an issue arose that could have been life-threatening for one of our students, a Bark team member called our school to help us take correct action."
>
> —Thad Schulz
>
> Technology Coordinator, Sebeka Public School District

The Importance of Digital Citizenship

Today's students are digital natives, having been born into a world immersed with technology. However, just because it's omnipresent in their lives doesn't mean they know how to use it as it was intended. Thoughtful and respectful engagement with technology promotes positive effects in the larger world, and it is an integral component of digital citizenship.

It's more important now than ever that students know not only how to use the technologies available to them, but also how not to use them. Only then will students be in a position to affect the kinds of change they hope to see in the world. In order to do so, every student needs to develop the digital citizenship skills that will help them contribute to their communities and make smart choices online and in real life. Bark for Schools helps facilitate the teaching of digital citizenship in the following ways:

- Teaching students the importance of accountability in online activity
- Enabling schools to monitor and ensure safety in the classroom
- Engaging the school community in important discussions regarding the intersection of technology and behavior
- Practicing online discretion with web exploration in an educational environment

Our Partners

Google for Education · Microsoft · National Center for Missing & Exploited Children · Police Foundation · Student Privacy Pledge Signatory · Crime Stoppers · Sandy Hook Promise

Visit our website at bark.us/schools for more information about Bark for Schools.

bark FOR SCHOOLS