The Administrator's Guide
to Bark for Schools

bark FOR SCHOOLS

Introduction
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 G Suite and Office 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 2,100 school districts across the country — with dozens more joining every month.

In 2019, Bark for Schools detected millions of concerning situations on school-issued accounts, including:

- **892,670** instances of children buying, selling, or discussing illicit drugs
- **251,367** students involved in cyberbullying
- **91,812** children expressing self-harm, cutting, and/or sucidal 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.

> Bark gives me the peace of mind that we have the capability of monitoring our students' online interactions and the convenience of staying informed to address concerns with individual students.

- Jocelyn Sotomayor

Upper School Principal
Holy Spirit Preparatory School

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, cyberbullying, 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 recurrent neural network?

A recurrent neural network (RNN) is a class of artificial neural network where connections between nodes form a directed graph along a sequence. RNNs 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 issue.

Our underlying network is based on a recurrent neural network (RNN) trained on custom word embeddings to aid in understanding the variations of childspeak. We 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 issues. 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 + PowerSchool

Schools can use Clever to sync family contact information by downloading the Bark for Schools app. PowerSchool users can also connect to the Parent Portal by integrating Bark for Schools into their unified information system. These features greatly simplify the onboarding experience for schools, removing the need to manually input data and allowing administration to spend their time on more important things.

Our free monitoring service can be up and running within minutes, and once schools have synced their accounts, Bark for Schools will begin monitoring student activities for potential issues. Schools can also choose which apps and accounts to have covered by Bark for Schools. The login credentials for these platforms are not stored by Bark but are used to establish our access to their online activities.

What We Monitor

Google Suite

- Drive: Photos, Videos, PDFs, Office documents, Plain text files
- Google Docs: Content, Images, Comments, Replies
- Gmail: Subject, Body, Attachments (images/videos), and Gmail Chat (text)

Office 365

- OneDrive: Photos, Videos, PDFs, Office documents, Plain text files
- Outlook: Subject, Body, Attachments (images/videos)

Google Suite and Office 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. Case in point: we've caught more than 60,000 instances of cyberbullying in Google Docs alone.

Chrome and Chromebook

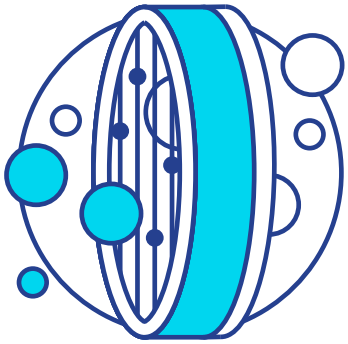
Our monitoring service provides a specialized browser extension for Google Chrome, which is the inherent browser on Chromebooks.
As Chromebooks are among the most popular devices issued to students in 1:1 districts, this extension allows Bark for Schools to monitor these browsers and devices with the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

The benefits of a built-in monitoring extension for Chrome cannot be understated. While students can log out of G Suite or Office 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.

G Suite

Office 365



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.

Security

Security is one of our highest priorities at Bark, and we adhere to all of the standards required by the Family Educational Rights and Privacy Act (FERPA), a federal law that protects the privacy of student education records. In an effort to provide maximum protection for students and their families, many states have adopted their own privacy legislation in addition to FERPA, and we meet or exceed each of these requirements, as well.

We secure all of our data within an encrypted database, including backups. The database is then purged after the data has been analyzed. Our server infrastructure is located in highly secured physical data centers that use a centralized bastion host, which is monitored to detect unwarranted access/activity. All web browser sessions use and require SSL encryption. And of course, no data is ever sold or given to any third party without consent.

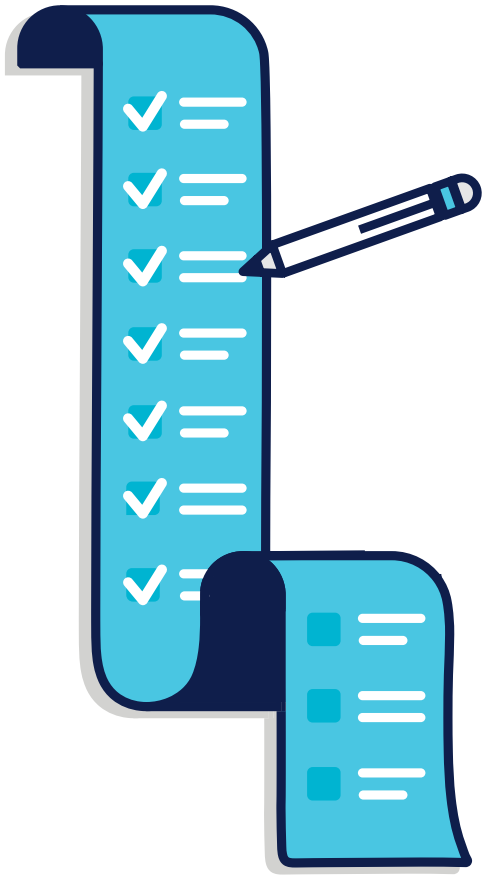
Monitoring Content Categories

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 issue is legitimate. If the Confidence Score is high enough, the alert will be auto-sent, notifying school administrators directly through the Bark for Schools platform.

Severity is the 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 "cyberbullying" 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 cyberbullying.



> Cyberbullying is a problem that schools struggle to control or even identify within their culture. Bark provides a way for schools to collaborate with parents in a proactive way to combat this issue and provide a safer environment for learning.

- Tim Hammill

Curriculum Services Director
Westmoreland Intermediate Unit

Abuse Types

Cyberbullying

Communications that indicate cyberbullying 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.

Suicide/Self-harm

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.

Grooming

Child grooming is a technique 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 use
- Alcohol use

> Bark's algorithm can identify coercive language and speech patterns used by adults, even when those adults are pretending to be children.

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 issues 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.

The capabilities of our algorithms are such that 99.4% of messages are not seen by human eyes. 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 and text 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 issue within that time, the Data Annotation team leaders send emails after judging that the issue is serious enough to merit the school's immediate involvement.

We highly recommend that schools have a designated person 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 issues — like a school shooting threat — are often time sensitive, so it's imperative that a contact is available. Issues 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.

> The capabilities of our algorithms are such that 99.4% of messages are not seen by human eyes.

Online Safety Compliance with Bark

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 safer 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 G Suite and Office 365. We also filter web domains at the IP 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 and web filtering
- ✔ Data stored in encrypted database
- ✔ Web browser sessions use SSL encryption
- ✔ Physical servers secured with centralized bastion host
- ✔ 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. Within a few days, Bark found multiple issues that would have gone unnoticed if we hadn't been scanning Gmail and Hangouts. 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

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

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

bark FOR SCHOOLS