

Kik's Unenforced Guidelines and Policies

Cover Page: National Center on Sexual Exploitation's Policy on Sharing Proof

WARNING: *The material in this document may contain graphic text, blurred images, and survivor quotes that may trigger the viewer.*

Why do we post proof in the first place?

NCOSE researchers have collected this proof as evidence of the material that is made, contained, and/or distributed by the corporations and institutions NCOSE is confronting.

Proof is shared with corporate executives, shareholders, and/or board members, as well as with policymakers, law enforcement, journalists, and the general public to **give witness to the sexual exploitation and abuse that is often rampant, yet sometimes hidden, on these platforms.**

Why do you blur out images, including faces, if they're publicly available?

While we believe it is important to provide ample evidence of wrong-doing to support our claims and inspire change, **we also strongly believe that no one – neither adult, nor child – should be exposed to the type of material our researchers collect:** either for their own well-being, or out of respect for those being exploited. It is for this reason we pixelate/blur/block not only nudity or sexually graphic content, but also the faces of those being exploited.

We also want to limit access to this material (unfortunately, a luxury not afforded to children and adults using many of the platforms and products made by these companies). Therefore, we add several layers before someone can access the proof, and also don't include all the proof that we have obtained. If someone feels they need to see more evidence to understand the extent of the problem or the type of exploitation that is happening, they may request it of NCOSE by writing to public@ncose.com.

Did you receive people's permission to post?

Any personal testimony shared to NCOSE directly is posted only with the affected parties approval.

For material that is publicly available, we do not seek permission to post. However, we redact names and usernames of survivors from articles, social media, etc. even when publicly available. To read more about our commitment to ethical engagement with survivors, please go [here](#). We do not redact names or usernames of exploiters who have posted publicly.

Disclaimer: while we do collect information on those who request access to more proofs, that information will only be used for our own, internal analysis. It will not be distributed, shared, or posted publicly or with outside parties.

Kik's Unenforced Guidelines and Policies

Kik has built its brand on being a “positive chat community” for everyone over the age of 13. The platform claims to be dedicated to fostering such a community, and provides resources such as a [Safety Center](#), [Parent Tips](#), and [Law Enforcement Guide](#).

In Kik's [Community Standards](#), they outline several rules about what is or isn't allowed on the platform, including “pornography and other inappropriate content.”

Can I distribute pornography or inappropriate content through Kik?

Nope. That includes sending, requesting, commenting on, linking to, or advertising inappropriate content.

By “inappropriate content” we mean any photo, video, or written depiction of pornography, nudity, real or implied sexual acts, graphic or gratuitous violence, and anything else that doesn't belong in a positive chat community with an audience age 13 and up.

They also claim to work with law enforcement when illegal activity takes place on Kik:

Can I sell things to other Kik users (including selling Kik accounts)?

While we admire your entrepreneurial spirit, we can't let you do this. It's a nope.

Can I do illegal things on Kik?

Hell nope.

It is against our terms of service to use Kik to break the law, to promote an illegal activity (including terrorism or organized crime), or to send sexual or inappropriate content involving anyone under 18, including yourself. If you do, we work with law enforcement as needed.

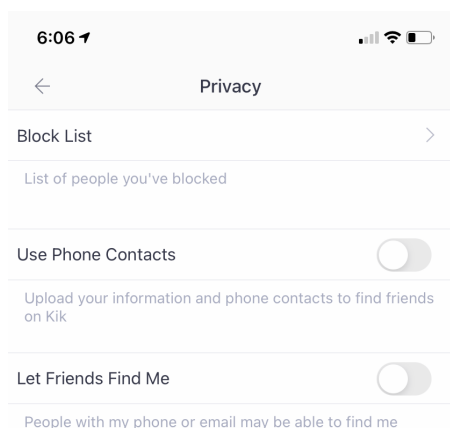
However, as detailed extensively in NCOSE research, Kik has completely failed to enact these policies as pornography and child sexual abuse is rampant on the platform. Despite Kik being aware of these issues for years, they still have yet to enact more stringent safety policies and moderation strategies to proactively catch and prevent this behavior from taking place on Kik.

Kik admits they have no obligation to monitor user activity in the [Terms of Service](#):

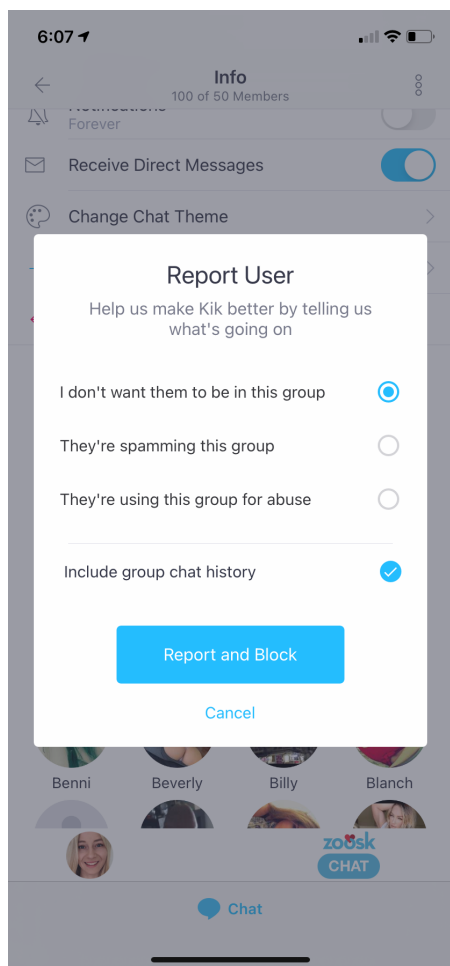
The Services offer users the ability to communicate and interact with one another. We encourage Users to treat each other with respect, and to understand that Users are solely responsible for their interactions with others. MediaLab has no responsibility or liability with respect to any online or offline interactions. We reserve the right, but have no obligation, to monitor interactions between you and other users of our Services. Please use your best judgment and keep safety in mind when you use the Services and interact with others.

This lack of moderation means Kik places the majority of responsibility on preventing and stopping bad actors such as adult predators preying on children on the users, who are 70% children themselves. The only safety features Kik provides is the ability to block or report another user – they currently do not have any parental controls, available filters, or other age-gates that would prevent the worst actors from contacting and accessing children online.

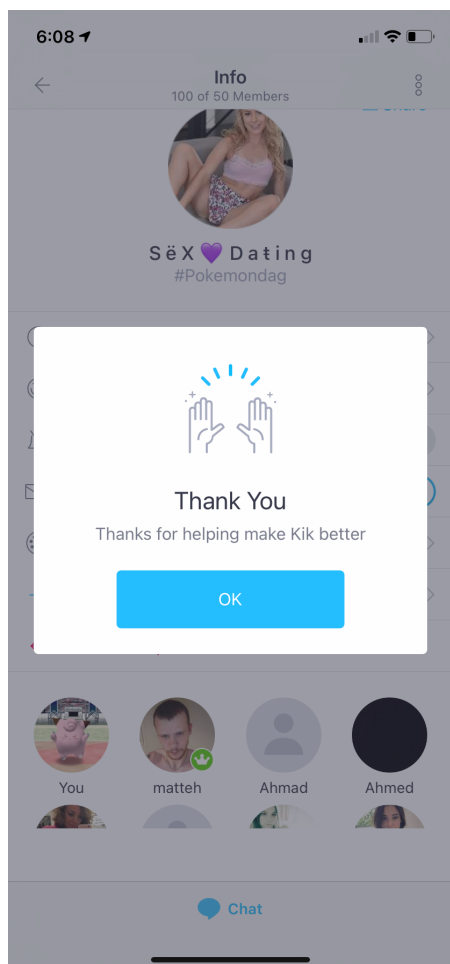
The available privacy settings on Kik (both options for phone contacts and letting friends find the account had to be toggled off manually, even as a 13 year old):



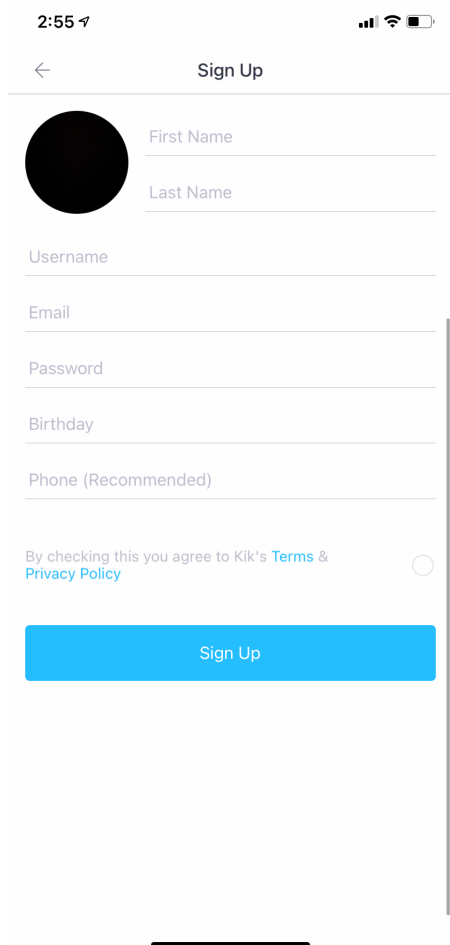
Kik offers a way to block and report individual users or entire groups:



Once a user or group has been reported using only the above categories, there is no other form or information intake. Users only see this message:



Kik does little to ensure users who have been blocked and reported stay off Kik – because the platform only requires an email upon sign-up, bad actors can make multiple accounts and continue to harass or target young users.

A screenshot of a mobile application's sign-up screen. At the top, the status bar shows the time 2:55, signal strength, Wi-Fi, and battery. Below the status bar is a navigation bar with a back arrow and the text "Sign Up". The main form area contains a circular profile picture placeholder, followed by input fields for "First Name" and "Last Name". Below these are fields for "Username", "Email", "Password", "Birthday", and "Phone (Recommended)". At the bottom of the form is a checkbox with the text "By checking this you agree to Kik's [Terms & Privacy Policy](#)". A large blue "Sign Up" button is positioned below the checkbox. A vertical line is visible on the right side of the form, and a horizontal line is at the very bottom of the screen.

Despite Kik claiming they work with law enforcement, their policies and procedures make it extremely difficult to do so. Law enforcement agencies around the world [have admitted](#) that Kik is hard to work with:

“Police say they are frustrated with Kik's response, with one detective saying getting information out of the firm was a "bureaucratic nightmare.”

Kik currently requires law enforcement to submit preservation requests using a specific [legal request form](#). However, several policies about data preservation make this process difficult and often fruitless.

Kik deletes content after a certain period of time has passed, and only stores chat data on the device it was sent or received.

Recent messages for each Kik chat are saved on your teen's smartphone (right in the app).

On your teen's iPod or iPhone with the latest version of Kik:

- For chats they've had in the last 48 hours, you'll see the last 1000 messages.
- For older chats, you'll see the last 500 messages.

On your teen's Android with the latest version of Kik:

- For chats they've had in the last 48 hours, you'll see the last 600 messages.
- For older chats, you'll see the last 200 messages.

If law enforcement wishes to investigate a user, they only have 90 days before Kik deletes the information:

How can I get account information for one of your users? What do I need to do?

7 months ago

The first step is to submit a Preservation Request using our [legal request form](#). We will preserve all available account data for 90 days. This will allow you time to secure a valid legal order.

If a user catches wind of law enforcement involvement or is otherwise removed or goes inactive, Kik only saves their information for 30 days.

If an account is banned OR inactive for over 30 days, could I still submit a preservation request?

7 months ago

No. When an account has been banned or is inactive for **more** than 30 days, there will not be any content data to preserve. Kik only retains content data for 30 days before it is permanently deleted from our servers.

Kik's lack of care in designing a platform that protects its majority userbase is egregious given the countless stories of grooming and clear evidence of pornography happening throughout the platform. And Kik's emphasis on privacy and data protection make it even more difficult for law enforcement to step in when needed, despite their claims otherwise.

Kik currently has policies on paper that in theory, bans sexual content from ever reaching users or taking place on the platform. However, it is abundantly clear that in practice, these policies are not enough to prevent the mass spread of illegal pornography, child abuse, and predatory grooming happening on Kik.