

LAW ENFORCEMENT GUIDE

Table of Contents

What is Kik?	2
Safety Features on Kik	3
Kik Identifiers	5
How to Locate a Kik Username	7
How to Locate a Kik Group Hashtag or Scan Code	9
Submitting a Legal Order to Kik	10
Available Data	11
Order Requirements and Recommended Language	13
Emergency Disclosure Requests	15
Preservation Requests	16
Additional Information	17

What is Kik?

Kik is a smartphone messenger application that lets users connect with their friends and the world around them through chat. Users can send text, pictures, videos and more – all within the app.

Kik is available for download through the iOS App Store and the Google Play store on most iOS (iPhone/iPod/and iPad) and Android (including Kindle Fire) devices. Users may also be using Kik on their Windows, Symbian-based or BlackBerry OS. As of May 2014, the download or registration of new accounts on Symbian and Blackberry devices is not supported.

Kik is free to download and uses an existing Wi-Fi connection or data plan to send and receive messages.

Using Kik

Kik is rated 17+ in the iTunes Store and Teen in the Google Play store. A user must enter their birthdate and be 13 years of age or older in order to register a Kik account.

Children under the age of 13 are prohibited from having a Kik account by the Kik Terms of Service. If Kik obtains knowledge that a user is under the age of 13, it's our policy to permanently deactivate their account and delete their personal information (unless otherwise notified by law enforcement).

Safety Features on Kik

<u>Usernames</u>

Unlike many other smartphone messaging services which are based on a user's phone number, Kik uses usernames as the unique identifier. By using usernames instead of phone numbers, users' personal information is never shared by Kik.

• Note: If a Kik user is an active user of other social apps and sites, they might choose to share their username on those sites to connect with their followers from there. Posting their Kik username somewhere like Twitter or Instagram, or on a Kik optimized webpage, will make it publicly available. This means people they don't know may be able to send messages to them.

Blocking Users

The 'Block' feature allows our users to block all contact with another user, without revealing to the other user that they've been blocked. Blocking someone means that messages from this user won't appear in the blocker's conversation list, and all previous conversations with this person will also be hidden. The blocked user's username will no longer appear in the blocker's list of contacts in Kik.

Blocking in Groups

If a user has been blocked by another, that user is unable to automatically add the blocker into a group on Kik. If a user is in a group with someone they have blocked, messages from the blocked user will appear as ***Blocked Message***.

Locating a Block List

In order to locate a block list, open the Kik app on the user's device and the main conversation screen will appear. Tap the 'gear' icon in the top left corner > tap Privacy > tap Block List.

New Chats

The 'New Chats' feature gives users control over who they talk to. This safety feature puts messages from new people into a separate section called 'New Chats'. In messages from new people, pictures or content messages they may have sent are blurred, with the option to unblur and view the content. A user has the option to either start a chat with them, delete, block, or report.

Reporting Users

If a user receives an unwanted message on Kik, they have the option to report that user. A user can choose to include a copy of their chat history with the in-app report, however, chat history is optional and is not required to report a user. A user can choose to report someone for the following reasons:

- They don't want to talk to them
- It's a spam bot
- The person is being abusive

Reporting Groups

A user can also report a group chat, if necessary. A user can choose to report a group for the following reasons:

- They don't want to be in the group
- The group is offensive
- The group is being used for abuse

A user can also choose to include a copy of the group's chat history with the in-app report, so long as they are a member of that group. If a user is not a member of the group but they still wish to report it, they will not have an option to include the group's chat history.

Kik Identifiers

Kik Usernames

- Unique
- Can never be replicated
- Can never be changed
- May include lower and uppercase letters, numbers and/or periods and underscores
- Will never contain spaces, emoticons or special characters

A Kik username is **the only publicly available identifier we can use to identify a Kik account.** We cannot identify users using phone numbers, first and last name (display name), or email address. We must be provided with the **exact** Kik username to conduct any type of search in our system.

Group Hashtag (Public Groups)

- User-generated hashtag
- Can never be replicated
- Can never be changed
- May include lower and uppercase letters, numbers and/or periods and underscores
- Will never contain spaces, emoticons or special characters
- The group hashtag will begin with a hash (#) (i.e. #KikIsAwesome)

Group Scan Code (Private and Public Groups)

- Can be accessed through the group profile information page (Info > Show Kik Code)
- Users can share the scan code to invite others to join

JIDs (Users, Private and Public Groups)

JIDs are unique internal IDs associated to users and group chats, randomly generated by Kik's internal systems. JIDs are not public-facing.

- A user JID is a username followed by an underscore and three additional characters that are randomly assigned by Kik for every username (i.e. testing_xs1)
- A group JID is 13-digit numeric string followed by "g". o it will not contain alphabetical characters (other than the "_g"), periods, spaces, or emoticons
 - i.e. 1234567891234 g

Content ID

A content ID is a unique ID associated to a media file sent on Kik. The format of a Kik content ID is eight alphanumeric characters, dash, four alphanumeric characters, dash, four alphanumeric characters, dash, four alphanumeric characters, dash, twelve alphanumeric characters.

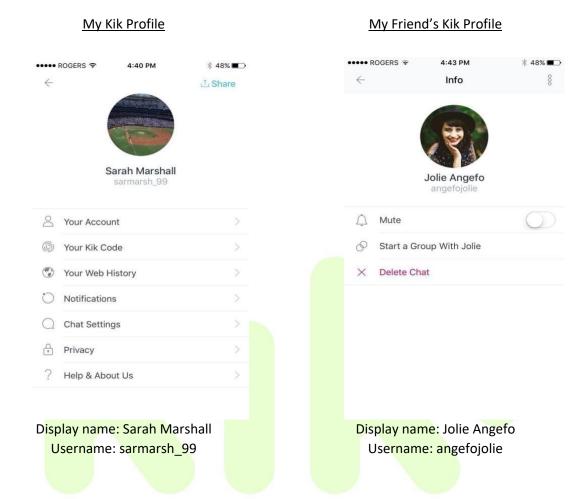
• i.e. ab1c2d3f-4gh5-6de3-9c88-e3f22fe25650



How to Locate a Kik Username

Tap the settings icon on the top left corner of device

In chat, tap the display name atop the conversation



There are two cases where a username may be unavailable on a Kik profile:

- 1. If a user has turned off their Receive Direct Message feature in a specific public group, their username will be hidden to other users in that group. This means that when you click on the user's profile, you will only see the display name and profile picture and no username.
- 2. If a user is chatting with someone in our Meet New People feature, their username, profile picture and display name will be hidden to the user they are chatting with for 15 minutes. After 15 minutes, if the users decide to become friends on Kik, their Kik profiles (including their username) will become visible.

If a user has used one of the above features, their anonymous username may appear in Roster Logs provided by Kik or in data obtained forensically from a user's device. The anonymous username is 52 characters long followed by an "_a" or "_b".



How to Locate a Kik Group Hashtag or Scan Code

Group Hashtag (Public Groups)



Group Scan Code (Private & Public Groups)



Group name: Camping Access the group scan code from the group Group hashtag: #arizonacamping information page > Show Kik Code

Submitting a Legal Order to Kik

Kik is located in California, USA, and as such is governed by United States law. We disclose account records and certain user non-content data in accordance with our Terms of Service and applicable law and must receive a legal order to consider disclosing content data in accordance with applicable law. This means to compel any user-data law enforcement is required to cooperate with the US federal, state, or local governments through an appropriate legal mechanism for the type of data being sought. Kik will only accept valid legal process (warrant or subpoena/summons) from a US federal, state, or local governmental entity or court. Further, Kik evaluates all requests as they relate to content or noncontent information.

Requests for information should be specific and include time frames. Broad requests for "all data" will cause significant delays in responding, and in some cases may mean we are not able to respond to your request.

Please use our Legal Request Form for production of all legal orders. Be sure to fill it out completely and upload any attachments at the bottom of the form. You may only attach one legal order at a time.

Preparing your Order

All legal orders must include the following:

- Addressed to Kik c/o MediaLab.ai Inc.
- Contain a valid Kik username(s) O Please see Page 6 for details on locating a username
- List of data requested o must be as described in this guide
- The method & timeline by which the disclosed data should be delivered to law enforcement Signature and date

Note: There are two exceptions where a username is not required in order to submit an order to Kik:

- The username of the subject account is unavailable as the user is using the Receive Direct Messages feature or the Meet New People feature
- The subject of the order is a Kik Content ID

Available Data

Kik's servers only retain images and video content for 30 days. When a user is banned or inactive for 30 days, all content falls off the servers and is permanently deleted immediately. Some content data logs may be available for a longer period of time, in alignment with our data retention policy and applicable law.

It's important to note that the text of chat messages **are stored locally on the Kik user's device**. We do not see, store, or have access to chat message conversations in our systems. The only exception may occur when a user reports abusive behavior using Kik's in-app reporting feature and chooses to send a copy of the conversation to Kik.

Non-Content User Data

- Basic Subscriber data
 - Current first and last name and email address
 - Link to the most current profile picture or background photo
 - If the user-account has been deactivated, the link to the most current profile picture or background photo will not be active
- Device related information
- Account creation date and Kik version
- Birthdate
- Email address used to register the account
- User location information, including IP address(es)
 - This information isn't verified by Kik, meaning we cannot verify its accuracy.

Content User Data

- Transactional chat log o Log of all the messages that a user has sent and received, including sender username, receiver username/receiver group JID, timestamps, IP of the sender and word count.
- This log does not include the actual message that was sent
- If the message was received by the subject user in a group, the log will contain the receiver group JID, not all receiver usernames
- Chat Platform Log O Log all the media files that a user has sent and received, including sender username, receiver username/receiver group JID, timestamps, IP of the sender, media type, and Content ID.
 - If the message was received by the subject user in a group, the log will contain the receiver group JID, not all receiver usernames
- Photographs and/or videos o Media files sent or received by the user for the last 30 days Roster log ○ Log of usernames added and blocked by the subject user, including timestamps.

- Abuse reports Transcript of reported chat history against the subject user, including sender username, receiver username, timestamps, actual message, and content IDs.
- Email events o Log of all the emails that have been associated with a username
- Registration IP o IP address associated to the username when the account was registered, including timestamp.

Content Group Data

- Group information log o Current information about the group, including the group JID, group name(s), group type, and the status of the group
- Group create log o Includes details about who created the group and at what time
- Group join logs A record of the users who have joined the group, including timestamps and the method that was used to join a group
- Group leave logs o A record of the users who have left the group, including timestamps and the method that was used to leave the group
- Group transactional chat log o Log of all the messages that a group has received, including sender username, timestamps, IP of the sender, receiver username(s), and word count.
 - this log does not include the actual message that was sent
- Group chat platform log o Log of all the media files that a group has received, including sender username, timestamps, IPs of the sender, receiver username(s), media type, and content ID.
- Photographs and/or videos o Media files received by the group
- Group abuse reports o Transcript of reported chat history against the subject group, including sender username, receiver username, timestamps, actual message, and content IDs.

Content ID Data

- First chat platform log related to a content ID o A record of the first time a specific media file was sent on Kik, including the timestamp, sender username, sender IP, receiver username/group JID, and media source
 - If the message was sent to a group, the log will contain the receiver group JID, not all receiver usernames

NOTE: We reserve the right pursuant to applicable law to refuse to provide information.

Order Requirements and Recommended Language

For Users' Non-Content Data (via US Subpoena/Summons)

- Basic subscriber data, unrestricted by date, associated to the Kik account 'USERNAME'
- IP addresses associated to the Kik account 'USERNAME'

For Users' Content Data (via US Warrant)

- IP addresses associated to the Kik account 'USERNAME' from 'DATE RANGE'
- All transactional chat logs associated to the Kik account 'USERNAME' from 'DATE RANGE' OR Transactional chat logs between the Kik account 'USERNAME' and 'USERNAME' from 'DATE **RANGE'**
- Images and videos sent and/or received between the Kik account 'USERNAME' and 'USERNAME' including the IP address associated to the sender of the images and videos from 'DATE RANGE' OR All images and video associated to the Kik account 'USERNAME' including the unknown usernames and IP address associated to the sender of the images and video from 'DATE RANGE'
- A date-stamped log showing the usernames that Kik account 'USERNAME' added and/or blocked from 'DATE RANGE'
- All abuse reports associated to the Kik account 'USERNAME' including the unknown usernames from 'DATE RANGE'
- All emails associated to the Kik account 'USERNAME' from 'DATE RANGE'
- Registration IP address associated to the Kik account 'USERNAME'

For users utilizing the public group "Receive Direct Messages" privacy feature or "Meet New People" feature

You may request the above data for users who have hidden their usernames with the Receive Direct Messages feature or Meet New People feature (i.e. "anonymous users"). If you know the anonymous username (52 characters followed by an " a" or " b"), you can use this username as the subject of your order. To identify an anonymous user without a username, provide the following information in your order:

- Note that the subject user is an anonymous user
- Username of the person who received the messages
- Date, timestamp, time zone of text messages received from subject
- Date, timestamp, time zone of media (photos/videos) received from subject user
- Display name of the subject user at time of chat o
 - O Note: if a receiver chatted with the user via the Meet New People feature, the display name and profile picture will not be visible to the receiver
- Public group hashtag (if applicable)

For Groups - Content Data

Group create log including the creator's username and IP address

- Group join logs from 'DATE RANGE' including the inviter and invitee username(s) and IP addresses
- Group leave logs from 'DATE RANGE' including the remover and removed username(s) and IP addresses
- Group transactional chat logs from 'DATE RANGE' including the senders' IP addresses
- Images and videos sent to the group including the sender's and receiver's usernames, and IP address associated to the sender of the images and videos from 'DATE RANGE'
- Abuse reports from 'DATE RANGE' including all usernames

For Content IDs – Content Data

The first chat platform log associated with 'CONTENT ID', including the username of the sender, the sender IP, the recipient username

Note: There is a difference between timestamps on messages in Abuse Reports vs. Chat Platform Logs/Transactional Chat Logs. Please be aware of this when requesting a timeframe for data in your legal order. If you are requesting data regarding a specific message or content ID, we recommend either:

- Widening the timeframe of your request so that it is not specific to a single second
- Requesting a chat platform log for a specific content ID sent by a user on a specific date



Emergency Disclosure Requests

For emergency cases involving the imminent danger of death or serious physical harm to a person, we have established an Emergency Disclosure Request process to allow the release of limited basic subscriber data.

Submitting an Emergency Disclosure Request

Please use our Legal Request Form for production. Be sure to fill it out completely and upload your Emergency Disclosure Request (EDR) attachment at the bottom. The EDR form can be downloaded from our Resource Center at https://medialabai.force.com/KikHelpCenter/s/topiccatalog/law-enforcement.

Once we receive your completed form, we'll review it. To prevent possible rejection, include as much detail as possible such as [potential] victim's age, custody, etc. If the investigation meets our emergency criteria, we'll provide the investigating officer with a Glossary of Terms along with the data response (if there is data available).



Preservation Requests

Kik may voluntarily preserve data, for a period of 90 days, upon receipt of a formal preservation request from a law enforcement agency. Kik's servers only retain images and video content for 30 days. When a user is banned or inactive for 30 days, all content falls off the servers and is permanently deleted immediately. Some content data logs may be available for a longer period of time, in alignment with our data retention policy and applicable law. We accept preservation requests from any law enforcement agency globally.

Submitting a Preservation Request

Please use our Legal Request Form for production. Be sure to fill it out completely. The EDR form can be downloaded from our Resource Center at

https://medialabai.force.com/KikHelpCenter/s/topiccatalog/law-enforcement.

Once we receive your completed form, we will review it and where applicable, will confirm preservation of data. Do not attach any other legal orders when submitting a Preservation Request.

Note: we will not be able to identify the username of the subject user without a valid US legal order.

Preservation Extensions

You can extend your preservation for an additional 90 days using our Legal Request Form. It is imperative that you check the 'extension' box and include the original preservation request Kik ticket or case number for reference.

This request must be made approximately one week before your original request expires. Upon review, Kik will extend the preservation for an additional 90 days, for a total of up to 180 days.

Note: If a preservation request expires, we cannot confirm that data still exists in our system.

Additional Information

Reporting Out

If we have reasonable grounds to believe Kik has been used to commit a child pornography offense, we'll file a report with NCMEC and/or the appropriate legal authorities.

Impersonation Reports

Kik users are encouraged to contact our Kik Support Team if they feel they have been impersonated on Kik. The Support Team will investigate the report and take action as appropriate. They may remove the profile picture from an account and/or deactivate the impersonating account. In the event the Kik Support Team isn't able to investigate or make a determination about an impersonation report, they may recommend that the user contact law enforcement for additional help.

Charges and Convictions

We invite you to let us know if an individual associated with a Kik username identified in your request is charged with an offense that involves unlawful or inappropriate use of our products or services. Upon receiving this information, we'll undertake an internal review of the individual's use of Kik and determine if removing the account from our platform is warranted prior to the prosecution proceeding to court.

Please also let us know as soon as possible if an individual associated with a Kik username identified in your request is convicted of an offense that involves unlawful or inappropriate use of our products or services. By notifying us, we'll be in a position to take appropriate steps under our Terms of Service. In most (if not all) cases, we will remove the individual's account from our platform.