

OCTOBER 2026



# NAVIGATING CONCERNING & ANONYMOUS ACCOUNTS

---

A Guide for Professionals



Copyright © 2026 Safer Schools Together. The reproduction of this material is strictly prohibited without the written permission of the copyright owners. All rights reserved.

**Disclaimer:** Given the rapidly evolving nature of technology and social media applications, this information (especially social media platform-related) is current as of the date of publication. This is an interactive document. Click the underlined links to read more or navigate to the correlating section of the document.

## TABLE OF CONTENTS

|                                                                                 |           |
|---------------------------------------------------------------------------------|-----------|
| <b>INTRODUCTION .....</b>                                                       | <b>2</b>  |
| <b>HOW TO LOCATE CONCERNING ACCOUNTS .....</b>                                  | <b>3</b>  |
| Key Considerations .....                                                        | 4         |
| Finding Accounts on Instagram .....                                             | 4         |
| Finding Accounts on TikTok .....                                                | 5         |
| <b>YOU HAVE FOUND THE CONCERNING ACCOUNT... NOW WHAT? .....</b>                 | <b>6</b>  |
| Best Practices for Reporting .....                                              | 6         |
| Reporting Impersonation Accounts .....                                          | 6         |
| <b>THE ACCOUNT WAS REPORTED AND IS STILL UP... NOW WHAT? .....</b>              | <b>7</b>  |
| Identifying the Possible Account Owner Based on Interactions .....              | 7         |
| <b>HOW TO IDENTIFY IF A STUDENT IS LOGGED INTO THE ACCOUNT OF CONCERN .....</b> | <b>8</b>  |
| How to Check on Instagram .....                                                 | 8         |
| How to Check on TikTok .....                                                    | 9         |
| <b>NONE OF THE STUDENTS OWNED THE ACCOUNT... NOW WHAT? .....</b>                | <b>10</b> |
| <b>CONCLUSION .....</b>                                                         | <b>12</b> |

## INTRODUCTION

Assessing concerning accounts can require significant resources for any school community. These accounts are often created and operated anonymously, making it challenging to identify the Subject of Concern (SOC) operating the account, as well as determining if the account presents a broader school safety concern. The content, behaviour, and connections associated with an account may also change over time, making timely documentation and assessment important. With a noticeable increase in concerning accounts, Safer Schools Together (SST) has developed this guide to support School Safety/Threat Assessment (SS/TA) teams in navigating the process of identifying, assessing, and responding to these concerning accounts. Its purpose is to help determine whether a SOC can be identified as the individual operating the account and, when that is not possible, provide practical and effective strategies for having the account reported and removed. This guide also provides a structured approach to help SS/TA teams assess available information, maintain appropriate documentation, and consider next steps within a multidisciplinary approach.

## HOW TO LOCATE CONCERNING ACCOUNTS

A concerning account is a social media account that shares violent, satirical, trend-based, or otherwise potentially concerning content. While some accounts may be created or perceived as entertainment, they may also be used to bully, harass, humiliate, or antagonize an individual, a school, or a broader community. Content may directly identify individuals or incorporate memes, GIFs, edited media, or current trends to ridicule, spread rumours, make accusations, or otherwise direct unwanted attention toward a person or group, often under the guise of humor or entertainment. In some cases, the account may appear to be intended as satire or humor while still contributing to a negative digital culture and climate within the school community.

Concerning accounts may come to the attention of School Safety/Threat Assessment (SS/TA) teams through reports from students, as well as from parents/caregivers who notice troubling content or interactions online. If these accounts remain unreported, they may remain unidentified and continue to operate for an extended period of time. This may make it more difficult for SS/TA teams to establish context, identify an account owner, document relevant information, and determine appropriate next steps. As a result, SS/TA teams should take steps to identify, document, and assess concerning accounts when they come to their attention, while considering the broader context and impact on culture and climate for the wider school community.

Best practice is for schools to proactively assess whether concerning accounts are connected to their school community, particularly those that may be causing harm, spreading rumours, or targeting individuals. SS/TA teams should have their members trained in [Digital Threat Assessment®](#) to develop the knowledge and skills necessary to identify and respond to concerning accounts. If members of your team have not yet taken the training, the focus should be on identifying accounts that reference the school's name, mascots, student groups, staff, locations, or other identifiable connections to the school environment. Concerning accounts may not be limited to just one single school; these accounts sometimes include an entire school district, geographic area, or broader community. There are several methods that can be used to identify concerning accounts, including keyword searches on Google, TikTok, and Instagram, as well as staying informed through student, parent/caregiver, and community reporting tools. Regularly revisiting these searches means SS/TA teams are best informed when seeing new accounts that may otherwise remain unnoticed.

Based on current trends and patterns observed at Safer Schools Together, these types of accounts are most often found on platforms such as Instagram and TikTok. Additionally, knowing some of the variations of these accounts can be helpful. The most common examples seen at SST are:

| Common Examples |                |                        |
|-----------------|----------------|------------------------|
| Bops            | Caught Lacking | Confessions            |
| Fight           | Goofs/Goofies  | Little Miss            |
| Opps            | Pisser         | Ship or Dip (Shipping) |
| Bathroom Snipes | Bathroom Shoes | Sleeping               |
| Slacking        | Bad Parking    | Gooner                 |
| Hotties/Hottest | People of      | Tea                    |

## **Key Considerations**

When navigating concerning accounts, SS/TA teams should use designated threat assessment accounts rather than personal profiles. An example of a threat assessment account would be the official school-based account. Youth are often highly aware of platform analytics and can see who has viewed, liked, or interacted with their content. Using a personal account can unintentionally expose a staff member's identity, increase risk, and, in some cases, contribute to an escalation of the concern.

Additionally, there is a growing trend of students locating staff members' personal social media accounts, saving photos or videos, and reposting this content to concerning accounts. In some instances, emerging Artificial Intelligence (AI) tools are also used to alter or manipulate these images, placing staff into false and/or disparaging situations.

For these reasons, maintaining clear boundaries online and using dedicated threat assessment accounts helps protect staff privacy, reduces potential targeting, and ensures appropriate navigation of concerning online behaviour. This approach also helps ensure that monitoring and intervention are conducted in a way that supports the safety and well-being of all who are involved.

## **Finding Accounts on Instagram**

To locate these concerning accounts on Instagram, begin by accessing the platform through a designated threat assessment account. One of the first areas to check is for any posts associated with your school's location, as this can often reveal worrisome online behaviours connected to your community.

To locate your school's geotag on Instagram, use Google, as other search engines may not yield the same results, and enter the following search:

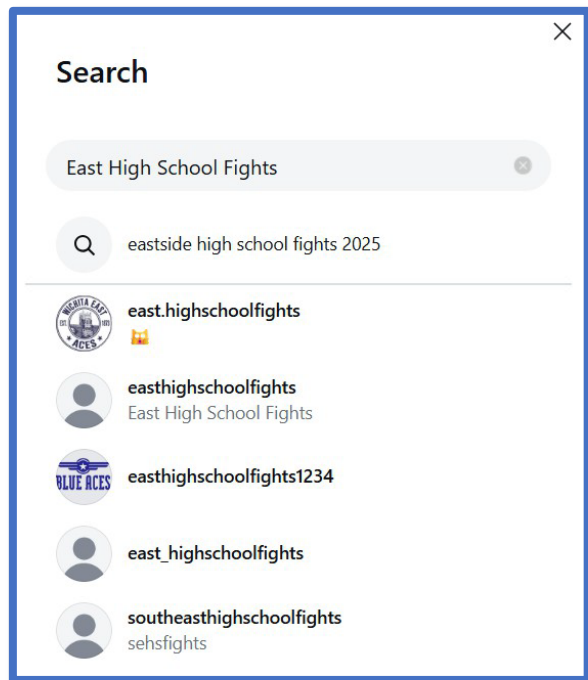
**site:instagram.com/explore/locations "SCHOOL NAME"**

If you do not see relevant results right away, try a few variations of your school's name. Once the geotag is located, you will be looking at "Top" posts and "Recent" posts. Top posts are the most popular, and Recent posts are in chronological order. This helps determine if there are any posts from these concerning accounts that have tagged the school.



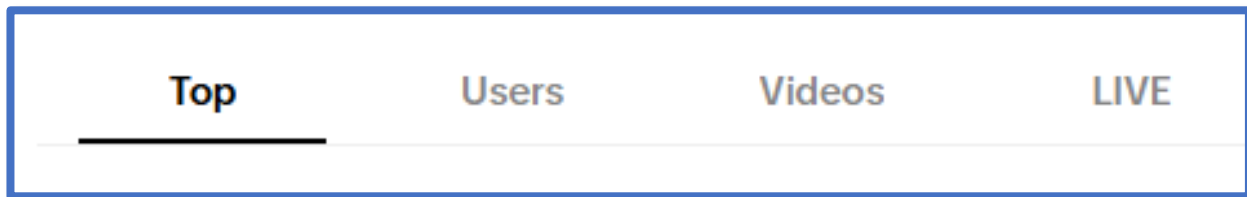
Another effective way to locate these accounts is by utilizing the [Instagram](#) search bar. Begin by typing in the name of the school, along with relevant key terms. This may help surface accounts that are directly or indirectly connected to your school community. As you review the search results, pay close attention to the profile image, username, logo, or other identifying information to ensure the account is associated with the appropriate school.

If the account cannot be easily identified, particularly when an account does not have a profile picture or other recognizable identifiers, review the followers and following lists. These accounts may be interconnected, where you may find links to other concerning accounts that contain recognizable school logos or identifiers. Additionally, review the content posted by the account to see whether there are indications of a connection to the school community, including references or interactions with identified youth that attend the school.



### Finding Accounts on TikTok

When searching for potentially concerning accounts on TikTok, the process may be more straightforward than on Instagram. TikTok's search functionality tends to have fewer restrictions, which may make it easier to locate accounts using school names, acronyms, and relevant key terms. By entering combinations of the school's name, school acronyms, and other relevant keywords identified earlier, SS/TA teams may quickly identify accounts that may be connected to your school community. To conduct this search, visit [TikTok](#) and navigate to the search bar. Enter the relevant search terms and carefully review the results under both the "Top" and "Users" sections. As results are reviewed, consider the available profile information and content to determine whether an account may be connected to the school community.



TikTok's algorithm may surface related content, meaning that once you engage with or view one concerning account, additional similar accounts may be recommended. This may assist SS/TA teams in identifying networks of accounts. In addition, this further reinforces the importance of conducting searches using a designated threat assessment account rather than a personal profile.

## YOU HAVE FOUND THE CONCERNING ACCOUNT... NOW WHAT?

Once a potentially concerning account has been located, the account and/or content should be reported through the appropriate platform's reporting process. While reporting may not always result in the immediate removal of an account or content once reported, it slows down the showcasing of this content on mainstream algorithms (for example, TikTok's For You Page). There are several considerations and recommended practices when reporting potentially concerning accounts or content.

### **Best Practices for Reporting**

- 1. Report the account from multiple IP addresses.**  
Submitting reports from different devices or networks increases the likelihood that the platform will recognize the issue as serious and act more quickly.
- 2. Avoid saying it is "someone you know"; instead, say it is someone you "do not know."**  
Reporting the account as an unknown individual encourages platforms to treat the report with greater urgency, as it makes the report increasingly objective rather than subjective.
- 3. If asked whether the concern involves youth under 18, answer yes in a school context.**  
Indicating that the account involves a minor ensures the platform applies stricter protections and prioritizes the report appropriately.
- 4. Provide additional context whenever possible.**  
Provide clear and relevant details to help platform moderators understand the severity of the issue. This may improve the chances of timely removal or intervention.

### **Reporting Impersonation Accounts**

Impersonation accounts are created to represent someone other than the individual operating the account. A common example we see is a SOC creating an account pretending to be a staff member of a school. When dealing with impersonation accounts on TikTok and Instagram, it is important to utilize each platform's dedicated impersonation reporting process. These reporting forms typically require providing specific information that shows the account is pretending to be someone else, such as matching usernames, photos, or content. Using the official impersonation reporting process can help ensure that the concern is prioritized and directed to the platform's moderation team. Include any evidence that supports your claim to speed up the review and removal process, but please note that the individual impersonated might need to provide official identification to the platform to verify they are the person submitting the report.

#### **TikTok Impersonation Report Form:**

<https://www.tiktok.com/legal/report/feedback>

#### **Instagram Impersonation Report Form:**

<https://help.instagram.com/446663175382270>

## THE ACCOUNT WAS REPORTED AND IS STILL UP... NOW WHAT?

Reporting a concerning account does not always result in the account or content being removed. Regardless of the circumstances, the account may continue to have a negative impact on the broader school community, meaning it must be addressed. At this stage, the focus may shift to identifying who is operating the account, as seeking voluntary removal of the account or content is typically the most effective and immediate method for removal.

### Identifying the Possible Account Owner Based on Interactions

The instructions below outline the exact methods that Safer Schools Together's Threat Analysts use to identify the owner of a concerning account.

**1. Open the account of concern.**

Start by accessing the account in question using a designated threat assessment account. Review the profile for identifying information such as the username, profile photo, and bio to verify this is the correct account you are trying to identify ownership of.

**2. Look at the first 5 posts shared on the account of concern.**

Focus on the account's initial posts, as these may provide information about individuals who are behind the account. In some cases, the account owner may engage peers to "like" and "comment" on the posts to generate engagement. Occasionally, the account owner may also interact with their own posts in this way, which can provide additional information about patterns of activity and involvement.

**3. Look through each post and note who comments and who likes.**

Review the interactions associated with each initial post, paying attention to the usernames of those who like or comment. This may help identify individuals who frequently engage with the account and who may have knowledge of its creation or support network. Document these names carefully for further review. Additionally, please ensure that the usernames are documented and not just the vanity/display names.

**4. Identify students who have a pattern of liking and/or commenting.**

Analyze the documented interactions for recurring usernames. Students who consistently like or comment on multiple posts may have closer knowledge of, or involvement with, the account.

**5. Bring those students in for interviews to determine whether they are operating the account or have knowledge of who is responsible.**

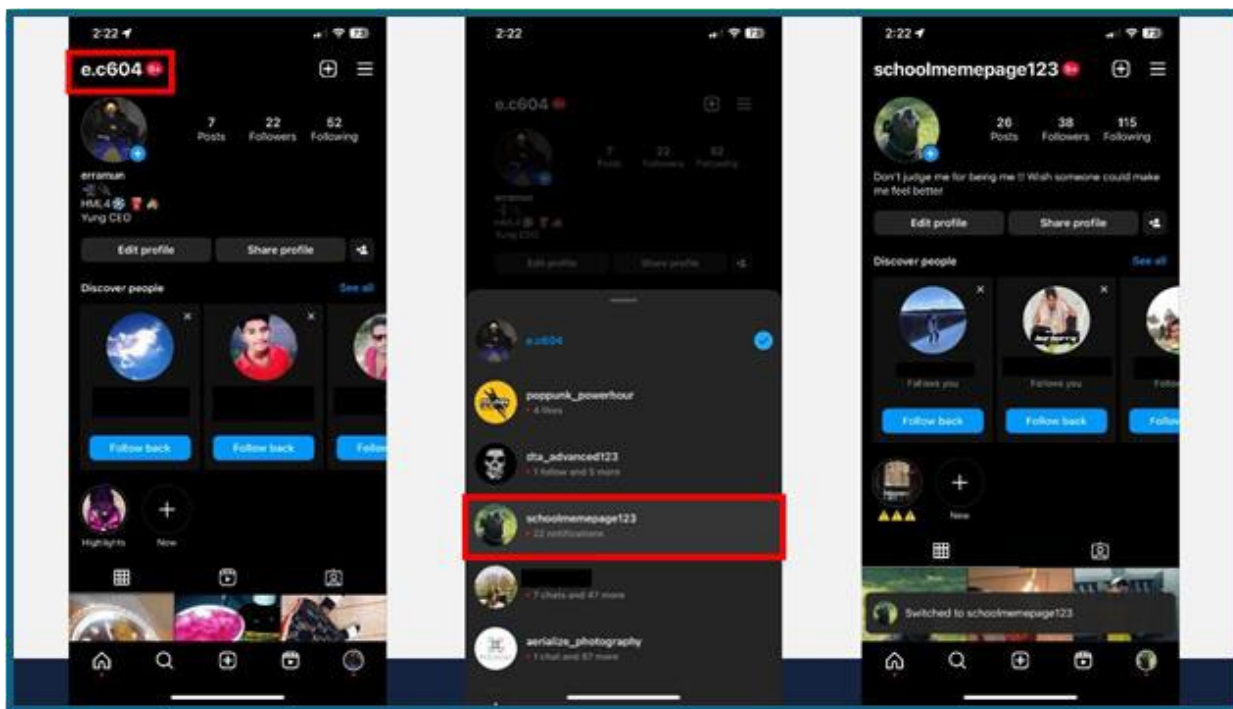
Once potential SOC's are identified, consider conducting interviews with these students, asking open-ended questions, such as, "Can you tell me more about this account?" The purpose is to gather information, clarify their involvement with the account, and determine whether they may be operating the account or have insight into the account owner's identity. If they are unable or unwilling to provide information that will support the investigation, review available information to determine if the youth is logged into the concerning account.

## HOW TO IDENTIFY IF A STUDENT IS LOGGED INTO THE ACCOUNT OF CONCERN

One useful feature of both Instagram and TikTok is the ability to identify whether a student is logged into multiple accounts simultaneously. This can provide additional information when assessing whether a youth may be connected to more than one account. The following section provides step-by-step instructions and accompanying graphics to support SS/TA teams in reviewing available account information and identifying students who may be accessing more than one account at a time.

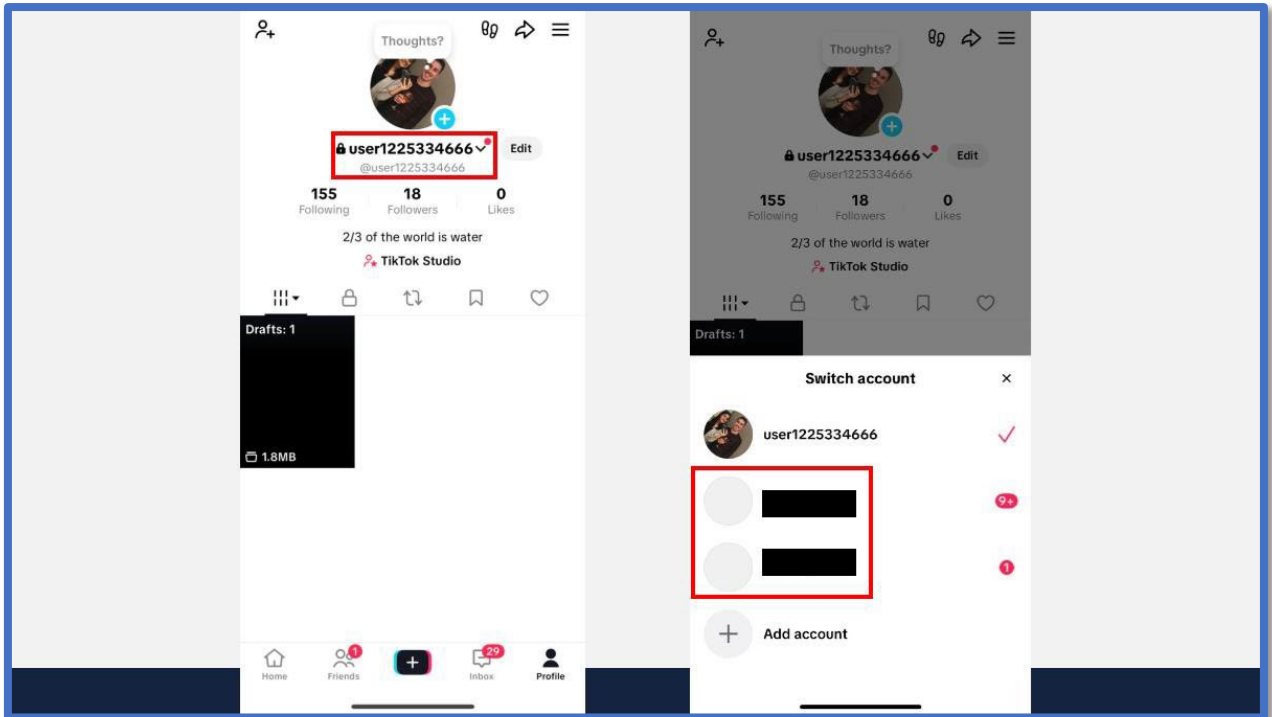
### How to Check on Instagram

- Open the Instagram app.
- Go to your profile by tapping your profile icon (bottom right).
- Tap your username at the top of the screen.
- A list of linked accounts will appear.
- Select the account you want to switch to.



## How to Check on TikTok

- Open the TikTok app.
- Tap the Profile icon (bottom right).
- Tap your username at the top of the screen.
- A menu will appear showing accounts that are currently logged in.
- Select the account you want to switch to.



If an account administrator is identified, the most effective way to permanently remove the account is by having the account administrator delete the account.

## **How to Delete Your Instagram Account:**

[https://help.instagram.com/370452623149242/?helpref=hc\\_fnav](https://help.instagram.com/370452623149242/?helpref=hc_fnav)

## **How to Delete Your TikTok Account:**

[https://www.tiktok.com/support/faq\\_detail?id=7543538137965058566](https://www.tiktok.com/support/faq_detail?id=7543538137965058566)

## NONE OF THE STUDENTS OWNED THE ACCOUNT... NOW WHAT?

If you have reviewed the account, identified students who frequently interact with it, and conducted interviews that did not yield any key information, do not be discouraged. There are additional strategies to address these accounts. Instead of focusing solely on identifying the individuals who may be operating the account, the next step is to engage the followers involved with the concerning account.

One practical approach is to provide communication to the parents/caregivers of students who are following the concerning account. This communication informs parents/caregivers about the concerning account and its impact on the school community. This helps raise awareness and encourages families to support the effort by discussing appropriate online behaviour with their children. It also serves as a reminder that following or engaging with harmful accounts may exacerbate the issue and that community-wide cooperation is essential to resolving culture and climate concerns.

SS/TA teams should first identify every student within the school community who follows the account of concern. Once identified, send a letter home with these students and request a parent/caregiver to sign the letter, confirming they have talked with their child. The signed letter should then be returned to an official at the school. Importantly, the letter should only be signed after the student has unfollowed the account.

The focus should be on reducing engagement with the account and reinforcing healthy digital boundaries, rather than assigning responsibility based solely on following or interacting with an account. Reducing the account's audience may decrease its reach, often leading to the account being deleted by the owner to avoid potential identification. Overall, sending these letters home to parents/caregivers is an effective strategy.

While the process can be time-consuming, it helps shift the school's culture and climate by reinforcing two key points:

1. SS/TA teams are actively monitoring for these types of accounts.
2. Students who choose to engage with concerning accounts will be held accountable.

An example letter template is provided below for your convenience.

**Sample Letter:**

*At [INSERT SCHOOL] we wish to uphold the values of our school community and code of conduct by ensuring that every student feels safe and secure when engaging in both our online and in our school community.*

*It has come to our attention that [INSERT NAME] has recently followed [INSERT PLATFORM] accounts that negatively impact the culture and climate of our school. I hope this letter will provide an opportunity for you to engage in a discussion with your child about establishing safe, caring, and respectful digital communities and being a helpful versus hurtful bystander.*

*Please ensure your child unfollows the following concerning accounts [INSERT ACCOUNTS] in an effort to have them removed from our online community.*

*If you could kindly sign this letter and have your child return it to [INSERT NAME].*

*Thank you for your cooperation regarding this matter. Please contact me if you have concerns regarding your child's involvement in this matter.*

## CONCLUSION

When navigating a potentially concerning social media account, a proactive and comprehensive approach is essential. By combining careful investigation, strategic reporting, and community engagement, including thoughtful communication with students and their families, SS/TA teams can effectively address these challenges.

Using designated threat assessment accounts for monitoring, understanding platform tools, and involving parents/caregivers helps create a safer and more supportive school environment. Remember, while removing these accounts can take time, persistence and collaboration are key to protecting your school community and fostering a positive digital culture.



SAFER  
SCHOOLS  
TOGETHER



International Center for  
Digital Threat Assessment