Security Guidelines

For Roller Derby Leagues

These guidelines are meant as a starting point for developing your own internal policies to safeguard your league, your members, and your fans. These must be adapted to how you run your events and what resources you have available to you. Not all of these suggestions may apply to your league. You are in the best position to make the determination on how best to protect your league and events.

Venues

1. **Risk Assessments.** Before developing your security plan, map out or outline current risks to the event. This includes:

    a. Site assessment - size and layout. Be sure to look for all entry and exit points throughout the venue and “blind spots.”

    b. Audience.

    c. Past event history.

    d. Current geopolitical factors.

    e. Local regulations.

    f. Known threats.

    g. Issues unique to your event.

2. **Security plan.**

    a. Have an authorized and permitted method of entry and exit from the event (eg. tickets plus identification, clear bags only for the event). Determine if further security is necessary for your event such as:

        i. Bag checks, wand stations, and metal detectors.

ii. Credentials for individuals who are authorized to enter and exit back areas such as locker rooms (e.g. staff and media).

iii. Determine if additional surveillance is necessary in blind spots or high traffic areas.

b. Have qualified, licensed, and sufficient security personnel for your event based on your risk assessment (above).

i. Outline roles and responsibilities of security personnel, security checkpoints, crowd control measures, and emergency protocols. Find out if any security are also trained in emergency response, such as CPR. If you are supplementing your security personnel with volunteers, make sure those volunteers are given direction by security personnel on how they can best help. Those volunteers should not be engaging with individuals and should be alerting the security personnel.

ii. Have security personnel clearly identified to the staff and audience, e.g. either through branded uniforms or other valid credentials and identification such as badges – this helps for finding them easily and also deterring threats.

iii. If there is a specific threat, such as any individual or group who will be present that represents a potentially heightened risk, make sure that information is communicated to security personnel prior to their arrival.

c. Have a communication plan in case of emergency, both from and to security personnel to your own league members/staff/volunteers, and to emergency personnel, and also to the audience. The communication plan should include how to communicate out that police or additional emergency personnel have been contacted and continued communications on their time of arrival, where people are to be directed if there is an evacuation.

d. Make sure all leadership, including visiting head officials, GTOs, head announcers are briefed on security plans and identify the person in your league they should approach with any questions or concerns during the event.

e. Have an emergency evacuation plan: Maps of emergency exits being well marked and unlocked (which can also be a consideration to the vulnerabilities for unauthorized entries). Make sure signage clearly directs crowds to those exits.

f. Have a general map of event flow/run-of-show for security personnel.

   i. If it's a tournament, have a daily meeting of leadership and include the person in charge of security to brief leadership on any security matters or adjustments.

g. Let security known where emergency personnel are and vice-versa.

3. Establish policies for vendors.

a. When making agreements with vendors, make sure they are aware of security and emergency plans that cannot be interfered with.

b. Have vendors disclose the number of individuals they will be using and provide credentials solely for that number. This can occur at the time of agreement or at their point of entry. For any change in personnel, such as in a shift change, have an agreement on how that will be done to make sure the right personnel are being let into the venue.

c. Vendors serving alcohol should have their personnel trained on overserving. This is generally necessary to obtain a license to serve alcohol to the public.

Social Media

While the upside of social media advertising includes that it's free to low cost, it has enormous potential reach, and it is fairly easy to involve your entire league and everyone in their networks in helping promote your events, all of that reach can also attract the attention of trolls and harassers. Unfortunately, advertising through social media always carries the risk of having to deal with trolls, harassment, and in some instances outright threats. There is no way to 100% prevent it from happening ever, but there are steps that can be taken to protect yourselves and your leagues, and to minimize the impacts. Hopefully these tips will help you in creating and managing your social media presence.

Create a social media policy. This will be important for either the succession of volunteers doing the position, or for any vendor you hire to do things on your behalf. Important to keep in mind if using a volunteer, social media can have an emotional impact, especially if you have attracted the attention of online harassers. Having a policy will help create a uniform response for a rotation of volunteers to give folks breaks when they need it.

1. **General security.**

    a. Perform an audit of all public facing information, this includes social media accounts and websites. Remove information that is unnecessary or reveals personal information. Don't publish personal emails for league facing contact.

    b. Limit access to social media to designated individuals. Have more than one person in leadership have access in order to retain control of the account and to grant and revoke permissions as needed. Revoke and grant access as needed. Highly recommend passkeys or multi-factor authentication (MFA).

    c. Don't use easily guessed passwords, eg. don't use your league name or someone's skate name and number.

    d. Don't reveal personal information of your leaguemates - government names, personal addresses, phone numbers, or emails. This includes being careful about inadvertently sharing personal information (e.g. creating media about a leaguemate's "day job" that reveals where they work) which can create security issues offline. It can also lead to trolls using that information to find your leaguemate online in other ways to stalk and harass. If a phone number is needed for whatever reason, don't use your actual phone number. There are a number of services that provide virtual phone numbers that forward to whomever needs to receive communications.

    e. Train/Inform your leaguemates on your social media policy and general social media safety so that they protect themselves. While not necessarily public figures, promoting events can put more of a spotlight on them. If they are sharing information on events and interesting stories to promote your league, they need to be aware of inadvertently exposing personal information about their leaguemates. This information tends to multiply exponentially with every individual that is sharing and promoting this kind of content to different audiences and reaches different corners of the internet. As part of your training, inform the league where they can report bullying, threatening and abusive behavior that happens online.

f. Keep up to date on technology. If your leaguemates have their own accounts that they do not advertise your league on, and are trying to keep their private lives separate, but their photos are appearing on your channel, facial recognition software can make it easy to find them; not just on social media, but across the internet - such as connecting the leaguemate to their LinkedIn Profile or a bio on a workplace website. Be up to date on privacy controls and how your posts can be shared. Inform leaguemates that they should be setting themselves to private if there is any fear of being connected to the league or an event.

g. "Delete Me" - there are programs out there that can scan for personal information and remove it from the web. This is one example of this type of program but there are others. Inform leaguemates of the service so that they can take control of their own personal information out there.

2. **Advertising.** Be aware that there are advertising rules and policies on social media but also regional laws. These are generally specific to your geographic area or if you are selling/promoting specific types of products. In the U.S. there are restrictions around advertising alcohol, tobacco, and firearms, but also items such as health supplements, CBD, medical devices, etc. This includes endorsing a product that is being sold by an advertising partner of yours. Be sure to do some quick research and if necessary consult an attorney versed in ad law to make sure you aren't committing some sort of civil or criminal offense in your advertising. You can be suspended from Meta platforms for running afoul of their policies but can also be sent a cease and desist from the Federal Trade Commission or your State Attorney General if you are committing any of these violations and they become aware of it. The bigger your reach, the more they will become aware of it.

3. **Harassment and Threats** - as part of creating your social media policy, you need to determine how you will respond to these and have a documentation system in place to keep track of them, in case they are needed for legal purposes.

    a. **<u>Don't ignore threats.</u>**

    b. Determine how you want to advertise on the front end, prior to publication of advertisements and how you want to allow your audience to interact with you. Part of that decision may include wanting interaction so that if there is a threat, you are made aware of it so you can document and report it. Options to consider are:

        i. Limit or disable comments.

ii. If allowing comments, either ignoring or monitoring and removing bullying and threats (this can require resources beyond what is automatically detected by social media systems).

iii. If allowing comments, blocking and when to escalate to reporting them.

iv. Limit and disable direct messaging unless from individuals who follow your accounts and then being able to block and report harassment.

c. **Criminal threats** - get to know your applicable criminal threats statutes. Every state in the U.S. and many countries and provinces around the world have one. It may have a different name, but there is likely a statute in your jurisdiction. If the threat meets the elements of that criminal threat statute, it should be reported to the relevant law enforcement in the jurisdiction that threat applies to. You should keep a record of those threats and when they were reported to law enforcement for your own purposes.

i. If the threat is to a person - that person should be informed and it should be noted by the league as part of the risk assessment plan for your venue security plan (see above). It should be reported to the police in the local jurisdiction that person is in.

ii. If the threat is to an event, the local police in the jurisdiction of the event should be notified.

iii. Determine whether a threat is sufficient enough to cancel or postpone your event. Usually if you report a threat with the details necessary to make a report, law enforcement will provide an opinion on whether you should cancel an event, or have law enforcement and extra security there with a briefing on the threat.

d. Documentation of threats:

i. Take screenshots or print out/scan and save to files. This will be important if something does happen. Make sure that record has dates and timestamps because those posts are likely to be removed by the offending party or automatically by social media platforms. Good documentation can help identify culpable individuals and also support evidence necessary for prosecution both civilly and criminally.

ii. Documentation is also important as it can help you keep track of the evolution of those threats over time. If the threats become more specific, more erratic, more threatening, you have a history to provide to law enforcement, especially if they aren't paying enough attention when you report it in the beginning.

iii. You can also use your documentation immediately with your security personnel at events in briefing them about potential issues. They should be able to review and assess any of those threats.

iv. Keep in mind the organization of your files should be in such a way that information can be found easily for presenting to law enforcement and security personnel, but secure enough from outside actors.

v. For retention questions: you should only remove documentation if you feel safe to do so. Generally inform anyone who would have been potentially affected by the threat prior to removal and get their consent to remove it. Otherwise, keep this documentation at a minimum for the statute of limitations as of the last occurring threat (usually 3-5 years). The statute of limitations will allow for aggregation of those threats backwards for evidentiary purposes. This means if you have a threat that occurred beyond the statute of limitations, but there have been more threats since the initial one, that oldest threat is still a consideration in prosecution. It usually is supporting evidence. So do not just remove the first threat in a string of threats at the expiration of the statute of limitations, if there were any after it.