Sussex Area Zoom Guidelines

Overview

These guidelines have been prepared for Sussex Area online meetings to provide information and practical advice for meetings that use a remote platform, specifically Zoom. Narcotics Anonymous has no affiliation with Zoom; however, Zoom remains a popular platform for our meetings.

This is a **local resource**. For additional guidance, please refer to NA World Services (NAWS) resources: https://na.org/virtual/

Introduction

There have been distance meetings available within Narcotics Anonymous for many years; these have been available through various online platforms and through telephone. They provide access to regular meetings that might otherwise be challenging for an addict. Zoom is a popular choice as each member attending can join through on open access link without registering or breaking their anonymity. This open access feature is what leaves our online meetings vulnerable to disruptors. These guidelines have been prepared to help technical hosts and secretaries of online meetings to navigate the security features of Zoom to keep the meeting safe. We cannot prevent disruptors from arriving in our meetings, we can however adopt processes that minimise the disruption that they create.

Sussex Area Zoom accounts

We have two Zoom accounts paid for by Sussex area and available for use for both recovery meetings and committee meetings. There is a timetable of use for each account and only one meeting at a time can be running in each account. It is important not to use the Zoom link outside of the time allocated to your meeting, time has been factored in for overrunning and early starts. If you use a Zoom account and wish to change the time or day of your meeting, please check with SAOC for availability on one of the Zoom accounts.

Title	**Associated email address**	**Logo**
NA Sussex Service	webservant@sussexna.org	universal programme logo 
Sussex NA Meetings	lsc@sussexna.org	blue QR code logo 

Security

Security is important to our meetings so that members and especially newcomers feel safe and feel that the meeting is well-run. As in face-to-face meetings, disruptions need to be dealt with in a firm and caring way. We make the following recommendations to assist with a smooth running of your meeting.

1. **Host Key**
   Sussex Area uses a host key system. Trusted servants who hold the host key should be

cautious about sharing it. Ideally, only two or three trusted servants (such as the meeting secretary and technical hosts) should know the host key.

2. **Roles and Responsibilities**
   For larger meetings, ensure there are enough trusted servants to manage the meeting effectively. Ideally, there should be:

   One person running the meeting (Secretary)
   One person providing technical support (Technical Host)

   Managing both roles simultaneously can be difficult, particularly when screen sharing. Make it clear to the meeting who members can message if they experience technical difficulties.

3. **Arrival Before Start Time**
   Waiting rooms are not automatically enabled, meaning anyone can enter the meeting before it starts. When a host key holder arrives, they should immediately claim host using the host key.

4. **Pre-Opening the Meeting**
   To minimise disruption before the meeting begins, a host may open the room well in advance (for example, 30 minutes or more), claim host, and enable the waiting room. They do not need to remain present; they simply need to secure the room and can return at the scheduled start time.

5. **Preventing Name Changes by Disruptors**
   Pre-opening the room and enabling the waiting room helps prevent disruptors from entering, observing member names, leaving, and re-entering using the name of a genuine member.

6. **Setting Security on Arrival**
   Once the host arrives for the meeting, they should:

   Enable the waiting room
   Review who is already present
   Confirm that those in the room appear to be genuine members or addicts seeking recovery

   Anyone suspected of being a disruptor can be placed in the waiting room or removed.

7. **Using Zoom Security Features**
   Each group is autonomous and may decide which security features to enable under *Host Tools*. Options include:

   Disabling chat or limiting it to host/co-host only
   Keeping all participants muted unless invited to share
   Preventing participants from changing their name
   Disabling screen sharing

   It is often good practice to begin with most options disabled and enable them only as needed.

8. **Managing the Waiting Room**
   Disruptors sometimes arrive in groups. Admit people from the waiting room **one at a time**, rather than all at once. Be cautious of unusual or inappropriate names, including those with double meanings.

If there are many unfamiliar people waiting, you may send a brief welcoming message explaining that they will be admitted shortly. This can sometimes prompt disruptors to leave voluntarily.

9. **Duplicate Names**
   Hosts should be alert to anyone arriving in the waiting room with the same name as someone already in the meeting. Be particularly cautious if someone appears to join, leave suddenly, and then return.

   If necessary, you may ask a participant to slightly amend their name if it duplicates someone already present. If admitted, monitor the participant and alert other hosts as appropriate.

10. **Reporting and Removing Disruptors**
    When removing disruptors permanently, only report them to Zoom if you are confident they are a disruptor. Reporting can result in bans that are time-consuming to reverse, and we want to avoid genuine members being excluded.

11. **Updates**
    The Zoom accounts are set to update automatically with any updates from Zoom. Do keep your knowledge current and consider attending a training webinar (free-of-charge) through Zoom.

Please contact SAOC if you think your host key has been comprised.

Any feedback or further ideas for this guidance gratefully received.

Sussex Area Online Committee

Webservant@sussexna.org

January 2026