

Nancy Elyse Grossman

From: bounce-124572474-76930839@list.cornell.edu on behalf of Shari Lynn Lighthall <slighthall@cornell.edu>
Sent: Tuesday, April 21, 2020 2:32 PM
To: NYFFA-L
Subject: Virtual Events - NY FFA

Tuesday, April 21, 2020

In today's new virtual world where collaboration and engagement needs to take place across several mediums and communication platforms, New York FFA wants to assure our teachers, parents, students, and administrators that the safety of our students and teachers is our first priority.

We recognize that many virtual platforms for online collaboration, meetings, and conferences have come under intense scrutiny over the past few weeks regarding their security protocols. Many companies have put additional security measures in place to protect the privacy of its users. These features only create a safer platform if they are actually implemented by the host of each event. When hosts are not responsible with meeting invitations, pass protections, or the enabling safety features, all online virtual programs regardless of the security features it may have are vulnerable to breaches.

At this time after weighing out all our options for the near future, we have decided we will be conducting our online events with the updated Zoom version 4.6.10 (with new security features) online platform. We selected Zoom, based on the Pro license obtained and recommended by Cornell University, the capacity for large meetings and webinars, the utilization of breakout rooms, and the newly enhanced security features. This newly released update makes meetings more secure and safe from Zoom bombing and phishing risks. Most notably, the update includes a new Security icon on the host's control bar, which consolidates many meeting security options in one place. Below please find the additional security protocols embedded that we will be using on all events to ensure we protect the privacy of our students and teachers who attend our upcoming sessions. The following measures will increase the security of our sessions and reduce the chance of unwanted attendees.

- **Lock Meetings**
When a meeting is locked, no new participants can join—even if they are authorized users or have a password.
- **Enable Waiting Room**
The Waiting Room feature allows the host to control when each participant joins the meeting and only allows participants to join if you specifically admit them after confirming they are supposed to be in attendance.
- **Rename Themselves**
We will prevent participants from renaming themselves in the meeting. We will ask attendees to enter their full name and no nicknames will be allowed. This will allow staff to confirm the identity of each individual and match it with the registration list of attendees.
- **Remove Participant**
We have the ability to immediately expel a participant from a meeting if they are not supposed to be in the event. The removed individual cannot rejoin the meeting.
- **Share Screen**
We will automatically turn this option off and prevent students other than the host from sharing their screens.
- **Chat**
With the enhanced security features we have the ability to turn this option off if necessary to prevent participants other than the host from using the Chat feature.
- **Annotate on Shared Content**
We will automatically have this feature turned off to prevent participants other than the host from using annotation tools such as Draw, Stamp, Spotlight, Text, and Erase when screen sharing is used.

- **Meeting ID's and Sharing of Meeting Invitation**

We will not share a meeting link publicly on our website or through social media. All registered participants will receive an invitation to join our meetings via email.

- **Require password for participants joining by phone**

When we have attendees joining by phone, we will require that they use a password to gain access to each event. Attendees joining by phone would not be visible by Zoom.

On 4.17.2020 we reached out to the NYS Education department, and below is the response we received regarding online video platforms and the utilization by CTSO Organizations:

As the ED Law 2d continues to change how districts and the like handle student information, a official guidance document is being constructed and will be released to allow for groups like the FFA to comply with this law. This guidance has not been released as of right now, and we are unsure what the timeline for release due to the current pandemic. For the time being, we are being told that these CTSO groups (FFA included) can act normally. At this current point, all we can provide is that there is no "right or wrong" platform, and the virtual platform that a district decides to use remains a local decision (per current guidance from the privacy office). Please note that Zoom among others is listed under the communication tools tab on the following link on the NYSED:

<http://www.nysed.gov/edtech/digital-tools>.

We understand that some of your schools may have established different protocols for the use of online instruction. We ask that you please share the above information with the newly established safety features that we will be using with your administration and IT staff at your schools.

Please reach out with any questions, I am happy to speak with any teacher, student, parent, IT staff or administrator to discuss this further.

All the Best,

Shari Lighthall, Director
Agricultural Education Outreach
Cornell University
607.255.9253, Ext. 4
slighthall@cornell.edu
<http://www.nysffa.org/>

