Safety Guidelines for 4-H Virtual Activities

For 4-H Parents and Guardians

Purpose of this document

The virtual landscape is ever-growing and fluid. A post shared between friends has the potential to be reshared across the globe through a wide array of platforms. Even if deleted from your account, your post may "live" forever on the internet. In our 21st century cyberworld, it is important to protect youth privacy and confidentiality. The suggestions found in this guide are intended to assist in keeping virtual interactions that youth encounter safe, appropriate and positive.

Expectations of 4-H parents and guardians, and 4-H members

When enrolling in 4-H, adults and youth sign a 4-H Code of Conduct outlining appropriate behaviors while engaged in 4-H activities and events. (**For liability purposes: Only youth who are enrolled in 4-H should participate in 4-H virtual activities.**) The behavior expectations found in the 4-H Code of Conduct apply in cyberspace, as well. A few of the key points from the 4-H Code of Conduct for youth to remember in all virtual interactions include:

- **Be inclusive:** With avatars and user names, it is easy to forget that we are interacting with people — other youth who have the same right to participate in 4-H virtual activities.

- **Be positive:** Even when your face is not seen, it is important to remember you are a representative of Missouri 4-H. Refrain from put-downs, negative comments, inappropriate content and profanity.

- **Be welcoming:** Through the internet, we have the opportunity to reach new audiences and invite them to join 4-H. It is important that your virtual presence, both live and recorded, foster a welcoming environment.

Safety guidelines for virtual activities

Encourage your 4-H youth to follow these general guidelines when participating in 4-H virtual events and while making recordings to share with others.

- **Overarching suggestions**
    - Talk about internet safety. Spend time online together to teach your kids appropriate online behavior.
    - Be aware of privacy and security settings available through your browser and online platforms. If you need assistance, use the Help pages that are typically available for browsers and social media platforms.
    - For younger children, keep the computer in a common area where you can watch and monitor its use, not in individual bedrooms.
    - Take your child seriously if they report an uncomfortable online exchange.

- **Internet browsing**
    - Check the privacy and security settings of your internet browser. Go to the Help or Support page for your internet browser to learn how. Suggested settings include:
        - Disable pop-up windows giving the user the option to open it or not.
        - While not 100% effective, block what the search engine would consider offensive or inappropriate content. For instance, most browsers allow you to block profanity.
        - Likewise, turn on Safe Browsing (if an option) to warn you of potentially harmful sites.
    - For youth 12 and under, consider bookmarking pages that are visited often or will be used for the 4-H activity. This reduces the risk of being misguided to a malicious site.
    - Check internet history, and make it known to your child that you plan to do so.

- **Social media** (Facebook, Snapchat, Twitter, Instagram, and similar content-sharing platforms)
  - Limit what identifiable information is shared on the youth's public profile. Showing only the youth's first name and a picture provides more anonymity than sharing last names, school names, etc.
  - Alternatively, restrict access to the youth's profile to "friends" only.
  - Send and accept friend requests only from known persons. Block unknown persons who attempt to follow the youth.
  - General safety regarding posts
    - In tagging photos, others should not identify youth to a greater extent than they identify themselves. Err on the side of caution: If a friend never tags themselves in photos, do likewise and do not tag them in your posts.
    - While sharing with others is part of the social media experience, use privacy settings to limit who can view content. Consider "friends only" or "friends of friends" over "available to everyone."

- **Web-conferencing and livestream**
  - General safety suggestions
    - Do not participate in private chats. "Private chat" is not completely private. The host of the meeting has access to all chats (even private ones) after the virtual meeting is over.
    - Limit what information is shared about the youth, especially if the livestream is to be recorded and shared later. Addresses, school names, telephone numbers and social media handles provide too much information about the youth.
    - 4-H recommends that youth under the age of 18 should use an account set up by their parent/guardian.
    - Be sure the youth knows the basics of how to mute and unmute their microphone and video.
    - Be sure the visible background in the child's video feed does not identify a child's location (for instance, a recognition certificate or poster with the school's name), and that it is appropriate.
  - Public, Open to All — Anyone with the link may join.
    - Livestream services such as Zoom allow you to rename yourself. Consider using first names only, especially if the youth appears on video. Do this upon entry, as hosts can turn off the renaming option once the livestream begins.
    - If video is optional and not requested, disable the video feed. Doing so may have the added benefit of reducing internet lag.
  - Closed, By Invite Only — Only those invited may join.
    - Follow the general safety suggestions (above) and consider limiting what information is shared, especially if the meeting is to be recorded and shared.

- **Recordings** (YouTube, recorded PowerPoints, and recorded livestreams)
  - Limit what information is shared about the youth.
  - Limit who has access to the recording:
    - YouTube gives you the option to set the video link to "unlisted" allowing for sharing the videos with friends while hiding the video from everyone else who visits your channel.
    - Cloud-sharing services (such as Box, Google Drive, etc.) give you the option to create a public link or restricted link. Restricted links give you control over who may view the recording.
    - Facebook gives you the option to share recordings with "friends", "friends of friends", or "public" depending on the level of security you desire.