Creating a Safe Live Virtual Club
Last Updated: 4/14/2020

During Club closures, many Clubs are turning to virtual platforms to deliver live programming to members. This is a great opportunity to build community, but it's important to think about your engagement carefully. Remember that no virtual platform is entirely safe.

This documentation covers what you need to know and steps that can be taken to make the virtual experience as safe as possible. Above all, staff and volunteers should continue to protect the safety and security of members by adhering to the organization's safety policies.

Enabling Safety

At a high level, building a live virtual experience requires shifting your thinking about safety from the offline context into the online context. That requires thinking about a few additional things, like data privacy, appropriate communications, internet safety, and what kinds of tools and practices you and your staff, as facilitators, will need to use or apply to ensure safe interactions online. Remember that your organization's policies related to background checks, supervision, communication, and prohibition of 1:1 contact must always be followed, even in virtual spaces.

Privacy and Security

- Review the platform's terms and conditions related to privacy and data collection.
- Select a platform that is age appropriate (note that some platforms have minimum age requirements).
- Look for platforms that are compliant with federal laws related to the privacy of children online, such as COPPA.[1]
- Quick tip: ask your local school system for their recommendations!

Conference Room Control

- Ensure your online sessions and/or groups are invite-only. Only a known audience should be able to participate.
- Ensure your online sessions and/or groups are password-protected and/or private. Use full capabilities to ensure your audience is limited to those you directly serve; also prevent "content-bombing," which occurs when an attendee intentionally shares explicit or other unwanted material with other participants by audio, screenshare or video.
- As your meeting commences, please ensure that you or a co-organizer can actively monitor online spaces to quickly remove and block any unauthorized users.
- Do not post links to your sessions in public places (physical or virtual).

Audio / Video

[1] More information on COPPA, or the Children's Online Privacy and Protection Act, is available here: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

- Make sure you have the ability to turn on and off (“mute”) audio / video capabilities for a specific participant or all participants at once.
- Do not ask children to participate via video unless you have express parent/guardian permission to do so. For members 13 and older, permission is preferred. For members 13 and younger, permission is required.

Chat communications

- Turn off participant-to-participant direct private communications, including chat feature among participants and members. This is essential to ensure a prohibition on 1:1 adult to member contact.
- Moderators should be able to turn on/off a public chat channel monitored by all.
- Moderators must be able to save an audit log of all member-to-moderator communication. This is essential to ensure a prohibition on 1:1 contact.

Parental Controls

- Enable content filters to block information, videos, or channels that you do not want a child to access.

Software Options

Your unique situation will determine which software best fulfills these and other requirements your organization may have. Popular options include, but are not limited to:

- GoToMeeting
- Join.Me
- WebEx – Standard
- Zoom – Professional Edition

Note: Free software plans come at a cost! Most typically, that cost is privacy and security. It is well worth a nominal monthly fee to ensure privacy and safety for your Organization, Club staff and members.

Please note that none of these platforms are 100% safe on their own. Be sure to explore the safety features of each platform and use supervision and monitoring tactics to fill gaps in the technology.

Secure Caregiver Consent

- Secure parent/guardian consent in **writing**. That can include hardcopy or digital submissions if the digital submissions are via online survey or form. Be sure that parents/guardians have read and consent to the platform’s terms and conditions related to privacy and data collection.
- Active (opt-in) consent is important; passive (opt-out) or verbal consent is insufficient. Gaining consent over the phone is not sufficient.
- Before interacting with members online, make sure that parents/guardians understand how the Club will use online platforms to interact with members and how they can support the process.
- Be sure to collect parent/guardian permission to collect and monitor electronic data about the member prior to recording any online interactions.
- Encourage parents/guardians to supervise members while online.

How to Comply with the Prohibition of 1:1 Contact

- Never interact with members one-on-one. This includes no 1:1 contact via online chats, direct messages, social media posts, phone calls, emails, and more.
    - Create a supervised virtual space that utilizes the rule of three (or more!).
    - Remember not to respond to, message, call, email, or communicate individually with any member before, during, or after the scheduled program time.
- Enforce appropriate communication by enabling/disabling platform features.
    - Enable chat logging for all chat communications but do not record youth in a session unless parents and caregivers have consented. You may record a session led by facilitators (featuring facilitators) for others to review.
    - Prohibit 1:1 contact between members themselves to limit personal sharing.
    - Prohibit file sharing by members.
    - Prohibit screen sharing by members.

Ensure Positive Community

- Begin each session by creating or reviewing group agreements. What are the expected norms for participation?
- Establish codes of conduct and guidelines for discussion.
- Provide internet safety training to participants prior to communicating online.
- Create a safe atmosphere.
    - Designate staff members to monitor interactions online.
    - Watch youth-to-youth interactions and keep an eye out for potential instances of cyberbullying.
    - If using video, be mindful of any items that may be in the background.
    - Select quiet spaces with little background noise and no distractions.
    - Ensure that any computers, websites, cell phones, or other software used for online programming have secure passwords that are required for access.
- Never use personal social media accounts.
    - Use official Club accounts to interact with members online.

Report Concerns Immediately

- Respond quickly to any inappropriate behavior online.
- Document incidents and report them to your supervisor.
- Remember that all Club staff and volunteers are mandated reporters.
- Report concerns confidentially:
    - Childhelp National Child Abuse Hotline at 1-800-422-4453

For additional support, contact:

- Praesidium Safety Hotline 1-866-607-SAFE (7233) or safeclub@praesidiuminc.com
- Ethics Point Hotline: 1-866-295-3701 or ethicspoint.com
- National CyberTipline, operated by the National Center for Missing and Exploited Children 1-800-843-5678 or erport.cybertip.org

Additional Resources

For more information on virtual and online safety:

BGCA resources

- BGCA.net/virtualprogramming
- BGC.net/cybersafety
- Myfuture.net

Outside resources

- CommonSense Media: www.commonsense.org
- National Center for Missing and Exploited Children: www.missingkids.org
- Darkness to Light: www.d2l.org/safe-digital-learning-plans

For more information on GoToMeeting:

- 5 Best Practices for Staying Secure in GoToMeeting: https://blog.gotomeeting.com/5-best-practices-staying-secure-gotomeeting/

For more information on Join.Me:

- Join.Me FAQs: https://help.join.me/joinmehelp/s/?language=en_US

For more information on WebEx:

- 4 Key Security Features of WebEx: https://blog.webex.com/video-conferencing/four-key-security-features-of-cisco-webex/

For more information on Zoom:

- Zoom Security: https://zoom.us/security
- PC Mag How to Prevent Zoom-Bombing: https://www.pcmag.com/how-to/how-to-prevent-zoom-bombing

Contact BGCA's Child Safety & Quality Assurance team for more information on ensuring safety in virtual programming: childsafety@bgca.org

For specific technical support for the platform you may be using, please contact the vendor directly.