Boys & Girls Clubs of Canada
Repaires jeunesse du Canada

Guidelines for Online/Virtual Club Programming

Version– June 4, 2020

Contents

1. Child Safety Risks in Virtual Programming

Boys and Girls Clubs provide a safe and supportive environment where children and youth can experience new opportunities, overcome barriers, build positive relationships and develop confidence and skills for life. Clubs are stepping forward in this unprecedented time in Canada's history to provide safe, accessible and innovative virtual programming for vulnerable children and youth. Now more than ever, the safe space, the relationships with caring adults and the supportive interactions with peer groups that are the foundation of Boys and Girls Clubs are needed for vulnerable children and youth across Canada.

2. Guidelines

2.1. Prohibition on 1 on 1 Contact

A prohibition on 1 on 1 contact between Club staff and members (or "rule of 3") lies at the heart of Clubs' child safety policies. This includes a prohibition on 1 on 1 contact at any time at the Club or outside of it. Some Clubs have exceptions to this rule for certain activities. To the extent that the prohibition on 1 on 1 contact applies to in-person interactions between staff and members, it must be maintained in online interactions. In order to enforce this rule, it is helpful to have staff sign off on the policy and to institute the supervision protocols outlined below.

Policy
1. Staff are prohibiting from communicating directly with individual members through digital means. They may not respond to, message, call, email, or otherwise communicate individually with any member before, during, or after the scheduled program time. Any individual communications must be directed to parents. This applies to all parameters of the programming (e.g. the sessions, the log-in information to access the sessions, etc.).
2. Communications to members must include a group of members or, ideally, all members.
3. Staff must use official Club accounts, and ideally Club-owned technology, to interact with members online. They are prohibited from using personal social media or email accounts. Communications must happen at appropriate times of day.
4. Staff must set appropriate restrictions to maximize the privacy on their own personal social media accounts, ensuring that Club members cannot view or post content. They must refrain from sending or accepting friend requests from members or liking content in members' personal social media accounts.

Supervision Protocols
1. More than one staff must be on all outgoing and/or incoming communications.
2. Where possible, for live/interactive programming, an additional staff or supervisor should be online monitoring the staff delivering programming. If this is not possible, consider how to ensure appropriate supervision of staff.

2.2. Caregiver Consent and Education

Caregivers can play a key role in protecting their children, and it is the Club's responsibility to equip them to effectively supervise their children's online interactions. Before communicating with members online, Club staff must secure parent/guardian consent in writing. Active consent is important; passive or verbal consent is not enough.
Make sure that parents/guardians understand how the Club will use online platforms to interact with members and how they can support the process. Parents/guardians should be told what the expectations and guidelines are around the programming and its delivery and how to report any concerns to your organization (472-1784 or programs@fbgc.ca or lisa.roy@fbgc.ca) . Be sure that parents/guardians have read and consent to the platform's terms and conditions related to privacy and data collection. 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.

Caregivers may be directed to https://protectkidsonline.ca/app/en/ offered by the Canadian Centre for Child Protection to learn more about helping their kids stay safe online.

2.3. Technology Protocols

No matter which technology platform is used, the Club must take steps to protect members' privacy and block access by any unauthorized users. Club staff should have a way to know the members in their session are part of their Club; their session is not open for young people (or others) to join. As a policy, Club staff should be sure the technology they select requires verified login (perhaps using e-mail address) and **allows them to see the full names of participants**.

Clubs can enforce appropriate communication by enabling/disabling platform features:
- Enable chat logging for all chat communications, but do not record members in a session. You may record a session led by facilitators (featuring only facilitators) for others to review.
- At the end of each session, a Club Staff must save a chat log to their computer (locally) to ensure an audit trail exists.
- Prohibit private communications between staff and members and between members themselves.
- Prohibit file sharing, screen sharing, and recording by members.

2.4. Creating a Safe Atmosphere

It is the Club staff's responsibility to create a safe atmosphere.

In the first session, establish member codes of conduct and guidelines for discussion. It is helpful to provide internet safety training to members prior to communicating online. Members should be told that at no point should they share any of the following via the live meeting: e-mail address, social media address(es) or locations to personal profiles, mobile number, or other personally identifiable information.

Staff must respond quickly to any inappropriate behavior online. They must document incidents and report them immediately. Staff should watch youth-to-youth interactions and keep an eye out for potential instances of cyberbullying.

Club staff should ensure the websites and/or other distance experiences they select are appropriate for their audience. Check all tools before messaging outward.

Practically speaking, if using video, be mindful of any items that may be in the background. Some platforms allow you to select a digital background, such as a photo or a logo. Select quiet spaces with little background noise and no distractions that is appropriate. Personal areas like bedrooms ideally and bathrooms should be off-limits.

Boys & Girls Clubs of Canada
Repaires jeunesse du Canada

Appendix 1: Zoom Meeting Information

Boys and Girls Clubs of America has vetted Zoom Meetings' Pro-level (which is what we will be using) service for its ability to provide distance-based experiences. Zoom Meetings is accessible to those who are on computers, tablets or mobile devices, and whose broadband varies in capacity.

What is it?

Zoom provides an opportunity to deliver safe video and chat-based educational experiences to members via any device.

How does it work?

Club leaders procure Zoom accounts for "hosts," or program leaders, to use. One "host account" will be required for each cohort experiencing virtual programmatic experiences together.

Members (children and youth) only require the basic level account with zero cost associated with it.

Family / Caregiver Responsibilities

Distance-based programming requires Club staff and youth to connect virtually, from their homes or wherever they can access a web or mobile-based connected experiences.

- Family/Caregiver Supervision. While a virtual experience can provide important activities and social connections, it does not provide childcare or guarantee physical safety. Families and caregivers should still plan for appropriate levels of supervision.

- Communication with Families/Caregivers. Club leadership should initiate the distance-based learning experience by sharing communications with families and caregivers about the opportunity to participate.

- At no point should youth share any of the following via the live meeting:

    - E-mail address

    - Social media address(es) or locations to personal profiles

    - Mobile number

    - Other personally-identifiable information

Data Privacy

When invitations are shared with your community, they should be shared to parents. Parents should load the experience for youth members. This ensures a minimum of youth data is captured or handled anywhere in the process.

Zoom Meetings' privacy policy can be found here: https://zoom.us/privacy

Zoom is utilized by school providers to connect with their students virtually and is FERPA compliant; more information can be found here: https://zoom.us/docs/doc/FERPA%20Guide.pdf

Prohibition on 1:1 contact

At no point should staff message members directly within the software. All chat should be logged and saved as an audit trail.

How do I get started?

Access Zoom Meetings and sign up for accounts. Access should be instant. Participating hosts should then download software to their devices (computers are ideal for moderation) and test a live meeting. Meeting links will be shared to parents through email.