SOCIAL MEDIA AND YOUTH PROTECTION

- Contact information on media and web pages should be adult leaders (or, better yet, use generic address forwarding to at least two adults)
- Don't post full Scout names on web pages or Facebook groups/pages
- Screen members joining Facebook pages/groups - ask questions and review answers
- Require moderation of posts to unit Facebook pages/groups

- **All youth protection policies still apply in an online environment.** Ensure you always have two-deep leadership for online activities and meetings. Our ban on one-on-one contact between an adult leader and youth applies to all interactions – whether in person, online, through a web conference, over the phone, via text, or in any other form. (but note exception to two *registered* adults for merit badge sessions - can be unregistered adult such as parent)
- All aspects of the Scouting program are open to observation by parents, and the BSA suggests parents take part in online activities and meetings.
- **Use business-oriented conference platforms that include good safety and privacy features instead of platforms with other primary purposes (such as gaming).**
    - Review the terms of service, safety and privacy features, and data collection policies of any platform you use, and review the BSA Digital Privacy and Social Media Guidelines linked below.
- **Regularly review and implement the latest security features of your chosen platform to avoid unauthorized visitors or other security issues in your meetings.**
    - Just as you put in place plans for the physical security of your meeting place, here are some tips to consider as you get started developing your own strategy to manage online security:
        - Use unique meeting identification numbers for each session.
        - Utilize password features for all meetings.
        - Do not publish meeting invitations via public forums and remind attendees not to pass along invitations.
        - Use "waiting room" features to manage letting individuals into your meetings - at least until you have second adult on board, then can disable.
        - Disable features that you will not need, such as screen-sharing by non-hosts, private chats, and whiteboards.
- **Do <u>not</u> record online activities/meetings that include youth participants.**
- **Recording of online activities that only involve adults:** New York is a one-party consent state. Pennsylvania is a two-party consent state.
- **Safeguard personal information.**
    - If you collect a person's personal information online—for example, through web forms used to register people for online meetings—then you should post a notice or disclosure at the point of collection describing how you will use the information. The notice should be conspicuous and written in plain English.
    - Meeting organizers must keep such information private and not share a youth's personal information with anyone except that youth's parent or guardian or the unit leader responsible for tracking advancements. For example, a merit badge counselor should not publicly post or otherwise show a roster with personal information of Scouts the counselor has worked with.
- **Collecting personal information from youth under 13 is not recommended.**
    - Do not collect personal information *directly from* youth under 13 years of age due to the parental notice and consent requirements under the Children's Online Privacy Protection Act ("COPPA"). You should collect any data needed from the parent or legal guardian only.

INTERNET SAFETY GUIDELINES for youth

- Keep online conversations with everyone in public places, not in email.
- Do not give anyone online your real last name, phone numbers at home or school, your parents' workplaces, or the name or location of your school or home address unless you have your parents' permission first. Never give your password to anyone but a parent or other adult in your family.
- If someone sends or shows you email or any type of direct message/wall post with sayings that make you feel uncomfortable, trust your instincts. You are probably right to be wary. Do not respond. Tell a parent or trusted adult what happened.
- If somebody tells you to keep what's going on between the two of you secret, tell a parent or guardian.
  Be careful to whom you talk. Anyone who starts talking about subjects that make you feel uncomfortable is probably an adult posing as a kid.
- Pay attention if someone tells you things that don't fit together. If one time an online "friend" says he or she is 12, and another time says he or she is 14. That is a warning that this person is lying and may be an adult posing as a kid.
- Unless you talk to a parent about it first, never talk to anybody by phone if you know that person only online. If someone asks you to call—even if it's collect or a toll-free, 800 number—that's a warning. That person can get your phone number this way, either from a phone bill or from caller ID.
- Never agree to meet someone you have met only online at any place off-line, in the real world.
- Watch out if someone online starts talking about hacking, or breaking into other people's or companies' computer systems; phreaking (the "ph" sounds like an "f"), the illegal use of long-distance services or cellular phones; or viruses (online programs that destroy or damage data when other people download these onto their computers).
- Promise your parent or an adult family member and yourself that you will honor any rules about how much time you are allowed to spend online and what you do and where you go while you are online.