Safeguarding Policy for Virtual Computing Sessions offered to brownies, beavers, cubs, scouts and explorers.

Overview:

We thought it was best to put a policy together to cover the safeguarding elements to these sessions to cover yourselves but most importantly us. We do have a separate safeguarding policy for our usual sessions that take place face to face and online. We will highlight some key points and how these will be addressed when we deliver the sessions. Our main aim is safety and to prevent harm. I am sure if we stick to the guidelines below your section will have a wonderful time but most importantly be safe! Can leaders introduce us as guests and set out the house rules. If individuals aren't adhering to those, they should be asked to leave by the leader overseeing the group during the workshop.

1. **Parents should be around.**

For best practice we would advise parents to be in the same room for the whole session when the beaver/cub joins the session via zoom. If it's a Scout or an explorer parents can drop in and out to make sure their child is okay etc.

2. **Zoom meetings should be password protected.**

When we organise a meeting, we will send out the link/meeting ID with a secure password to make sure its those authorised to access the meeting.

3. **Waiting room activated.**

When we host computing activities for a section, we will have the waiting room activated and expect them to arrive a few minutes before. We will make the leaders present in the room a co-host and they would be in control to let their cubs and anyone they don't recognise they would remove from the waiting room.

4. **Participants need their webcams on.**

Participants needs to make sure their webcams are on just to make sure it is them and not somebody else pretending to be them. Its to make sure we are safeguarding others in the virtual room.

5. **Recording group sessions.**

We would prefer to record sessions if the group has permission for everyone just in case anything did happen it has been recorded. – In terms of GDPR the files would be password protected. Only the host/co-host should have access to record sessions, and no one should have access to that feature.

6. **Sharing Screens.**

Only allow the host and co hosts to share so have this feature disabled for others but if we wanted a participant to show what they have done we could allow that individual to share.

7. **Breakout rooms.**

Breakout rooms are a good resource if you have the correct ratios in each one. You need to have at least two leaders per breakout room. If you don't have enough leaders to cover the main room/breakout rooms don't use the breakout rooms during the virtual computing sessions. If the leaders why not? Explain the reasons why you can't.

8. **Physical surroundings.**

Making sure you are in the correct environment and dressed sensibly. Making sure you make family members aware you have a call and to be cautious and dressed appropriately if they need to enter that speafic room.

9. **Making sure Zoom has been updated.**

Make sure you are checking for the latest update of Zoom to keep everyone else safe. If you discover there is an update, make sure you alert your section. (Making sure any updates are installed)

10. **Meeting ID and Password.**

Ideally trying to send out the Meeting ID and then the password separately to the section so if a stranger does get hold of the meeting ID and password they can enter but you must make sure the waiting room has been enabled and with a recognised name so the host knows who it is to let them in. – For example, Meeting ID via email and the password via What's App to be extra secure.

11. **Locking the meeting.**

When everyone has arrived and when approximately 5 minutes have lapsed making sure the host locks the meeting so no one else can enter either the meeting nor the waiting room.