***Some youth groups are venturing into the virtual world to meet at this time. It is important that we keep in touch with the young people that we’re serving and this in itself can be a key way to support and safeguard some of our most vulnerable young people particularly during difficult and challenging times such as the current Covid-19 pandemic. Video conferencing and virtual online platforms are exciting tools but there are some genuine reasons why we have avoided this in the past including our awareness that there are additional risks and challenges in doing this in a safe and transparent way and also the fact that the internet is a context where much abuse has happened as it is seen to be difficult to manage.***

***Even at times of crisis it is important that these gatherings operate within our*** [***safeguarding policy and procedures and follow some clear safeguarding and good practice principles.***](http://www.paneldiogelwch.org.uk/images/5._Section_3.pdf) ***The work should always be transparent and safe and careful consideration given to the safety of the young people and the accountability and protection of the workers/ volunteers.***

**PRINCIPLES**

1. **Permission and consent and GDPR**
* Any work we do with children under 18 needs the specific and informed consent\* of their parent or guardian. Don’t assume your existing consent form covers new activities. Don’t rely on young people to communicate what is happening to their parents.
*\*e.g. An email sent to parents/carers which explains what you are doing, the date and time of the video conference session, which youth leaders are participating and what you roughly will be doing. Create a new consent form or ask for a reply as a form of consent and keep these emails in a separate folder. Use parents/carers email address to ensure parents/carers are aware that it is happening and can set up the young people to access the session appropriately with any oversight they want.*
* Never record any virtual session and do not post pictures of anyone under 18 unless specific permission is given. (i.e. using usual photo protocols)
* Apply Data Protection principles and GDPR rules to any data/ contact details.

**2. Careful preparation and risk assessment**

* *Risk Assessment:* as with any activity in church with children or young people, video conferencing / use of social media should be properly [risk assessed](http://www.paneldiogelwch.org.uk/images/Completing_a_Risk_Assessment_notes_and_form.pdf). Identify the risks and carefully note how you intend to mitigate or manage the risk.
* *Check and follow* [*age guidelines*](https://www.childnet.com/blog/age-restrictions-on-social-media-services): Most social media platforms do not allow children under 13 to hold an account. (See table A below) and some parents may not allow their children access. All modes of communication used need to be transparent and safe and parental permission sought.
* *Choose the platform carefully* e.g. ensure secure, group communication where people can only join with the consent of the administrator. Avoid the use of Skype / Facetime – these are social media tools and as such share contact details with all users, you may inadvertently connect young people with other people as an unintended consequence. Instead use a video conferencing platform such as Zoom. Avoid Houseparty as it is not a secure platform and it is not possible to manage attendees and Snapchat as messages disappear and it is not possible to provide accountability.

**3. Recruitment / lone working**

* *Recruitment*: As with all other work with children and young people, we should ensure that those involved in the work have been safely recruited and DBS checked where eligible. Appropriate training, including safeguarding training should be accessed and those who ar leading in any social media content use in the church should be confident in its use and alert to the risks.
* *Avoid lone working*: two adult leaders should be present in the virtual group from the start of the call (first to join, last to leave).

**4. Safe Practice**

* *Reporting concerns* .Be clear with young people that if they share something on social media that makes you concerned for them or another person you will have to pass it on, in line with the [church safeguarding policy.](http://www.paneldiogelwch.org.uk/en/advice-and-support)
* *Codes of conduct and ground rules*: appropriate behaviour for leaders and youth should be followed as you would expect in the usual youth group setting.
* *Maintain boundaries:* Do not use your personal social media account but rather set up an account for the youth group. Do not use social media to communicate with individual young people. Involve parents in the communication.
* *Model healthy social media use:* Do not post or respond to messages late at night
* *Church/ all age activities or services:* always consider the principles of consent and GDPR in terms of images and email addresses for all involved of all ages. If any events/ services are to be uploaded or shown online ensure all involved are aware and that you are not inadvertently publishing images of children or anyone without their permission.

TABLE A

|  |  |
| --- | --- |
| **PLATFORM**  | **MINUMUM AGE** |
| **FACEBOOK** | 13 |
| **INSTAGRAM** | 13 |
| **TIKTOK** | 13 |
| **TWITTER** | 13 |
| **WHATSAPP** | 16 |
| **GOOGLE HANGOUTS** | 13 |
| **SNAP CHAT**  | Do not use app where messages disappear as no accountability or protection |
| **HOUSE PARTY**  | Not a secure platform and not possible to manage attendees |

**USEFUL LINKS**

Safeguarding vulnerable groups handbook section 3 and 3.3A and D <http://www.paneldiogelwch.org.uk/images/5._Section_3.pdf>

visit the online safety page on the Panel website for more information and links

<https://www.paneldiogelwch.org.uk/en/on-line-safety>

Youthscape and 31:8 Creating safer places online. Guidance for communicating and working safely with young people online. 03/2020 <https://thirtyoneeight.org/media/2588/guidanc-for-online-youth-work_v3.pdf>

<https://www.youthscape.co.uk/podcast/virtual-youth-work>

Thinkuknow <https://www.thinkuknow.co.uk/>is a resource which has advice for children, parents and workers about keeping safe in the online world;

[Net Aware: Your guide to social networks, apps and games (net-aware.org.uk)](https://www.net-aware.org.uk/)

Childnet International <https://www.childnet.com/> has resources including a toolkit for parents and carers;

The Panel gratefully acknowledges the use of the online resources produced by the Church of England and Baptists Together in the preparation of this factsheet.

<https://www.baptist.org.uk/Articles/569876/BUGB_Guide_to.aspx>

<https://www.churchofengland.org/sites/default/files/2020-04/Video%20Calling.pdf>

Medi 2020

Example risk assessment.
Can be adapted to reflect a local situation

|  |
| --- |
| **ACTIVITY TO BE ASSESSED /CAUSING CONCERN : Youth meetings using ZOOM** |
| **RISK ASSOCIATED WITH THE ACTIVITY** | **Who may be harmed and how** | **CONTROL MEASURES** | **By Who** **and When** | **Complete****Y/N** | **Level of****Risk now** |
| **Security/privacy issues related to use of Zoom software.**Uninvited / unknown person gaining access to the meeting Using Personal Meeting ID to host public eventsUnauthorised recording of sessions ( Zoom has record facility) | Children and young peopleUnintentional facilitation of access to young people by 3rd party This creates a continuous meeting – anyone can access.Host and participants record meeting  | * leader to access online zoom training to become more aware of facilities and features and potential hazards
* Avoid publishing links on social media or in public forums –Date, time, and link to meeting to be shared securely.
* Both parents and participants to be told not to pass on link details to others Other interested parties must be directed to Activity leader as appropriate.
* The leader to compile list of participants before meeting and check attendees at the start of every meeting. Any discrepancy must be resolved before the meeting can progress.
* switch off in account settings prior to inviting participants
* No consent for data to be recorded, switch off in account settings.

Ensure all participants are aware that the session must not be recorded by any person. | Leader / organiser Before start of meeting then ongoing  |  | low |
| **Risk of inappropriate online contact/grooming or allegations**  | Inappropriate use of Zoom platform or contact on other electronic platforms Misuse of private message facility/ chat during a meeting  | * There must be two adult leaders present and visible within the session at all times. If either adult has to leave early the session should end.
* Both leaders should have undergone safer recruitment/DBS check for their role and safeguarding training. (additional safeguarding young people online training is desirable)
* Group meetings only rather than 1:1. No join before host setting enabled. All parties will be made aware that 1 to 1 session are prohibited. Ensure Screen sharing is restricted to host.
* Chat is turned off before start of meeting
* Leaders must complete Safeguarding Course. and are aware of the procedure to follow should a child make a disclosure.
 | Leader / Organiser Before and Ongoing |  | low |
| **Lack Of Parental Presence/Consent**  | Allegations of inapproprite contact with childrenPoor accountability | * Share details of meeting including purpose/ leaders and basic rules with parents/ guardians prior to meeting and obtain email consent.
* Advise that an adult is present in the room with the child at the start of session and ideally during the session.
 | Leader / Organiser Before meeting |  |  |
| I**nappropriate sharing of personal information/contact details**  Inadvertently providing access to personal information Inappropriate clothing/setting for sessions  | Sharing of personal information verbally, through messaging or through details visible in background of camera. Using Facebook to log in - access to personal information. Participation in meeting while wearing inappropriate clothing or in inappropriate location  | * Housekeeping at the beginning of each meeting advising against oversharing of personal information ie addresses, etc. Adults should ensure that they are in a neutral space without personal information visible and scan each screen window at earliest opportunity to identify any inappropriate / sensitive background etc
* Parents to ensure that the background area is free from personal items like family photos, links to address etc.
* Parents to ensure they have set up the zoom account via their email address not Facebook. Sign in using email address.
* Clear guidelines to attendees on wearing suitable clothing and suitable location for accessing meeting
 | Leader / Organiser andParents of Participants |  | Ongoing  Low  |
| Assessment completed by : JE can be adapted to suit a local setting | Date: June 2020  |