MED Theatre
Inspired by Dartmoor

MED Theatre Safeguarding Policy for Online Work

Updated Aug 2022

This policy will be updated annually

Contents

1.Introduction

This policy is in addition to MED Theatre's current Child Protection and Safeguarding Policy, and has been prepared in response to changes in practice due to social isolation during the Covid-19 emergency which began in Britain in March 2020. This policy has a specific focus on MED Theatre's use of the Zoom platform as all other platforms that the company are using were already in regular use before the changes in practice (eg. Facebook, Instagram, WhatsApp, etc).

2.Safeguarding Policies and Procedures for Virtual Meetings

● It is MED Theatre's responsibility to inform parents / guardians of under 18s of the risks involved with using any new online platforms. The parent / guardian needs to give permission for their child to take part in activities on these platforms. A guide of the wording to send to parents / guardians in advance of using Zoom is as follows:

For this (these) online session(s) we will be using the Zoom platform. There have been a number of reports in the press where inappropriate material has appeared out of the blue in the middle of Zoom meetings, and concerns have been expressed about Zoom's security generally. Having taken advice from various external organisations and individuals, we believe that Zoom has addressed many of these issues with heightened security measures. We also find that it is the most user-friendly online platform for our work. We want to make sure in the light of the above information that you are happy to use it with us. We will assume that if you click on the link to join the online session that you are giving your consent for your child to use Zoom.

This guide would also apply in the case of any other digital platform we had not been using previously and about which we were aware of security concerns, but still needed to employ for whatever reason.

● A minimum of two responsible adults in young people's virtual sessions at any one time

● Remind participants not to record or take photos of anything without the other participants' consent

● If someone else is visible/audible in the background on someone's screen ask the participant make sure that person is aware that the virtual meeting is taking place, in case they don't wish to be seen/heard

● Record and action safeguarding concerns in the same way as face to face contact; be transparent with the young people about this

● Lock and password-protect meetings

● Make sure a meeting host monitors the participants list and ensures no unknown participant joins. Unauthenticated users should be held in a waiting room so the organiser can check their identity before admitting them to the call.

● Enforce encryption by default and makes sure it's end-to-end if possible

● Be aware that audio-only participants calling via a regular phone dial-in option will "break" the encryption

● Be careful with meeting recordings and get consent from the participants

● Be careful with file and screen-sharing capabilities. They could accidentally disclose sensitive information or be used to spread malicious programs.

3. Responding to Disclosure received online or via mobile phone

We recognise that it is possible participants might disclose information to staff members via texts, calls or digitally. If a staff member receives a worrying message that they think may indicate that the young person communicating with them is at immediate risk during or outside of work hours, they should immediately refer it for action to the Designated Safeguarding Officer (Abby Stobart). The Designated Safeguarding Officer will follow the standard procedure. If the staff member cannot get hold of the Designated Safeguarding Officer and **they are concerned for the immediate safety of the child, they should alert the emergency services by calling 999**. They should write up any such incident report within 24hrs.