



Thread and Press CIC

Online Safety Policy

Updated 26.01.21

Online Safety Policy

Updated 26.01.21

Our aims are to protect all children, young people and adults involved in our organisation and who make use of technology (such as mobile phones, games consoles and the internet) while using our services.

We also aim to provide staff and volunteers with policy and procedure information regarding online safety and inform them how to respond to incidents. We also aim to ensure our organisation is operating in line with our values and within the law regarding how we behave online.

As part of using the internet and social media, our organisation will:

- understand the safety aspects - including what is acceptable and unacceptable behaviour for staff and children - when using websites, social media, apps and other forms of digital communication
- be aware that it doesn't matter what device is being used for digital interaction, but that the same safety aspects apply whether it is a computer, mobile phone or game console
- when using social media platforms, ensure that we adhere to relevant legislation and good practice
- regularly review existing safeguarding policies and procedures to ensure that online safeguarding issues are fully integrated, including:
 - making sure concerns of abuse or disclosures that take place online are written into our reporting procedures (See our Adult and Children's safeguarding policies)
 - incorporating online bullying ('cyberbullying') into our anti-bullying policy
- provide training for the person responsible for managing our organisation's online presence

Managing Our Online Presence

Our online presence through our website or social media platforms will adhere to the following guidelines:

- All social media accounts will be password-protected, and at least 2 members of staff will have access to each account and password and the account will be monitored by a designated person or persons
- The designated person managing our online presence will seek advice from our designated safeguarding lead to advise on safety requirements

- A designated person will remove any inappropriate posts, explaining why, and informing anyone who may have been affected
- Any social media groups will be set to private
- Any adult-only groups shall be monitored to ensure that we do not admit members under 18 for safeguarding purposes
- We will not contact children directly through our social media pages or platforms. The only exception would be a children's social media group. Children would only be admitted to this group with permission from parents and must adhere to social media age restrictions.
- We will never publish a child or adult's personal information online, including address, school name or telephone number. We may publish a photo or name but only with the permission of the adult, carer or parent.
- Any posts or comments will be consistent with our aims
- We'll make sure children, young people and adults are aware of who manages our social media accounts and who to contact if they have any concerns
- Parents will be asked to give permission and approval for us to contact children directly through any social media account or group, or by any other means of communication outside a specified and booked Online session.
- Parents will be asked and must give written permission for photos or videos of their child to be used by us in any online or printed format. We would also ask any adult for their permission before using photos or videos online.
- All of our accounts and email addresses will be appropriate and fit for purpose

Our Zoom Policy

Our online sessions are run through a licensed Zoom account. We provide Zoom meetings links and a passcode. Sessions can only be accessed with this link.

Staff and participants should never share these codes with anyone else.

Children's sessions will have a unique link and passcode for each session.

We do not allow screen shares for participants (only staff) in our children's sessions

We reserve the right to remove any participants of behaviour is inappropriate

We do not allow any recording of our Zoom sessions, unless by the host and only with permission from all participants

Any recorded footage provided by staff should not be shared with anyone outside of the session.

We ask that participants turn their cameras on for our sessions. Refusal to turn on a camera for introductions in our children's sessions may result in a place being terminated. This is simply to register and verify participants.

We ask that participants do not share any personal information in our sessions.

The host will end the call for all participants at the end of the session.

The host will ask participants to join a waiting room at the start of the call and the host will admit participants.

We ask that, if possible, participants change their screen name to match the participant's name.

What We Expect from Staff (including Volunteers)

- All staff will be aware of this policy and behave in accordance
- All staff communicating to children or vulnerable adults online will have an up-t-date Enhanced DBS check.
- Staff will seek the advice of the Designated Safeguarding Lead (Sarah Rands) if they have any concerns about the use of the internet or social media
- Staff should communicate any messages that they wish to send out to children, young people or vulnerable adults to the designated person responsible for the organisation's online presence (Holly Davis)
- Staff will not friend or follow children, young people or vulnerable adults from personal accounts on social media, or from personal email addresses or by private messages
- Staff will make sure any content posted is appropriate for the age forum of the group and for all ages when posted in the public domain
- Staff should refrain from communicating with parents through personal social media accounts wherever possible, and refer to formal communication methods using an organisation's email address, social media account or by telephone.
- Staff will never contact children, young people or vulnerable adults directly by telephone.
- If staff need to contact children via email, we would only do so with parents permission and we will copy at least one other member of staff into any emails sent.
- Staff will never contact children or young people directly outside of normal office hours
- Emails and contact will be signed off in an an appropriate and formal manner
- Any disclosures of abuse reported through social media will be dealt with in the same way as any face-t-face disclosure, according to our reporting procedures (see our Adult and Children's Safeguarding Policy)
- Smartphones will be used appropriately and will not be used to record any images or share any content without the permission of parents/carers. Content shared would meet our guidelines for appropriate content.
- Staff and young people would never engage in any inappropriate contact via online or other means.

What We Expect of Young People and Adults

- Adults and children should be made aware of this safety policy and agree to its terms before signing up to our courses
- We expect children, young people and adults' behaviour online to be consistent with these guidelines when using our services.
- Bookings for our sessions should be made only by an parent/guardian or carer with parental authority.

Using Mobile Phones

- Staff will not keep children's or young people's phone numbers and will make all telephone contact through a parent, guardian or carer.
- We would always seek parental permission if we need to contact children directly
- In the event of contact being made to a child with parent permission, a copy of all communication will be kept and provided to our organisation and provided to parents or guardians at their request. The purpose for any contact will always be made evident.
- If any child or young person makes contact with one of our members of staff via mobile phone (or other online device) we will either:
 - end the conversation and cease reply
 - suggest contacting the matter in a face-to-face or parental authorised event
 - if we are concerned for the child's welfare we will refer to the Designated Safeguarding Lead (Sarah Rands)
- We ask parents to advise children and that adults in our sessions follow the following when in our sessions:

- that mobile phones or recording devices should NOT be used in our sessions, online or otherwise. They should not be used for taking photos or videos in the session, sharing information from the session (whilst the session is in progress) or for communicating any information about others within the session
- That the use of mobile phones during a taught session would be considered inappropriate for children and we encourage children to only bring mobile phones to sessions for emergency use only
- We do not tolerate any bullying or discrimination, including that by mobile phone or other device. Please see our anti-bullying policy in our Terms and Conditions

Use of Other Digital Devices and Programmes

The principles in this policy apply not matter which current or future technology is used including computers, laptops, tablets, web-enabled games consoles and smart TVs - and whether an app, programme or website is used.

If any digital devices are used as part of activities within the organisation:

- we expect children and young people to adhere to the guidelines above
- we will ensure all staff adhere to the guidelines above