STUDENTS ORGANISING FOR SUSTAINABILITY UNITED KINGDOM

SOS-UK SAFEGUARDING ADDENDUM

This document is an addendum to the NUS Safeguarding Policy, and Social Media Policy, and provides guidance on how SOS-UK staff and volunteers should apply these polices in the SOS-UK setting. It provides additional safeguards that are required owing to the difference in the nature of NUS' and SOS-UK's work and operations, in particular online working and regularly working with young people under the age of 18 years.

1. Terminology

O18 - over 18

U18 - under 18

AAR - Adult at risk (previously known as 'vulnerable adults')

Core staff – Adult staff team that are not student staff

DBS – Disclosure and Barring Service

2. Social media (see social media policy)

- In accordance with the Social Media Policy, O18 staff and volunteers should consider whether it's appropriate to private message U18s. A lower risk option could be keeping communication in a public sphere using specified communication channels (e.g Slack threads rather than direct messages). If an email needs to be sent to an U18 it should be done from a centralised SOS-UK account, rather than a private email account wherever feasible.
- In accordance with the Social Media Policy, O18 staff and volunteers should consider whether it's appropriate to 'friend' or follow U18 staff and volunteers on their personal social media accounts. The exception to this is LinkedIn, due to U18s being able to use it for their professional endorsement. Employees and volunteers can mitigate risks by avoiding sending direct messages and reporting any inappropriate behaviour to the safeguarding team.

3. DBS checks (see safeguarding policy)

- **Before working with U18s/AAR internationally**, or hiring staff in other countries to work with U18s/AAR, the recruitment lead should research local vetting procedures and discuss a safeguarding plan with the safeguarding team. This is to check for any potential criminal convictions that have any potential risk to others we work with.

- **All UK O18 staff must be DBS checked before lone working with U18s/AAR staff or volunteers.** Depending on the nature of the project, if volunteers, trustees or contractors who supervise, care for or otherwise have significant direct contact with U18 or AAR, they will also need to be DBS checked.
- Professional one-on-one meetings such as regular staff/manager one-to-one's (121s) should be kept to a minimum, and it is recommended that the frequency should be once every three weeks at most. Instead of 121s, one-to-three's (123's) or one-to-four's (124's) are preferable i.e. group meetings. Under no circumstance should an O18 core staff member meet with an U18 volunteer in a personal capacity outside of work, and O18 volunteers and student staff should consider whether it's appropriate for them to do so.

4. Induction / at start of role

- Both U18s and O18s staff and volunteers must sign our Volunteer and Staff Agreement before being given access to SOS-UK organising spaces (e.g. the Mock COP26/SOS-UK/TtF Slack) and should have an orienting meeting with a core staff member.
- Emergency contact details to be collected at start of contract/volunteering for all staff and volunteers.
- All staff and volunteers must attend compulsory online safety and safeguarding training. Core staff must also attend an annual refresher training. (Note - this training is currently found on Workrite, but SOS-UK plan to develop in-house training).
- Parental/guardian consent is required for U18 staff and volunteers*. The consent form outlines all likely types of activity the role involves and will give details of the safeguarding practices, which will be in place, as well as contact details for the safeguarding lead.

  **In the event that an U18 is unable to gain parental consent, the safeguarding team will work with them to assess their options for participation. For anyone aged 16-17, alternative measures may be able to be put in place on a case by case basis. For anyone under 16 the reality is that their involvement with many of our campaigns may be limited due to our safeguarding responsibilities.*

5. Running a project/campaign with U18s/AAR

- Key project/campaign activities should be assessed to identify safeguarding risks and mitigations which can be made to reduce these risks. The assessment should be shared with the safeguarding team.
- It is the project/campaign core staff leads' responsibility to check all regular volunteers fulfil SOS-UK's safeguarding requirements.
- The complaints policy, as well as the contact details for the safeguarding lead, should be clearly communicated, on at least a three-monthly basis, to all staff and volunteers.
- Staff and volunteers should be supported to manage their workload or involvement in campaigns/projects to actively avoid burnout, or negative impacts on other areas of their life. Communications and decision-making structures should encourage this, e.g. if the team is voting on an important decision, there should be enough time allocated (e.g. a week at

minimum) for input and feedback, so staff and volunteers don't feel they have to be 'constantly plugged in' when not working/volunteering. For example, considerations should be given to annual leave, public and religious holidays, personally priorities.

6. Planning an online meeting or event with U18s/AAR

- Online meetings should be set so that attendees need password/secure link to enter the session, and it should be made clear that these details must not be shared.
- When feasible, online meetings with U18s should be set up with two core staff in attendance as support, observer or facilitator. Core staff should be available to support with, or deliver sessions/meetings, and monitor behaviour and chat, etc. to ensure online meetings are safe spaces for all.
- Staff should only use organisational accounts for online platforms (e.g. Skype or Zoom) and make sure no personal info is accessible, ie personal email or phone number.
- If U18s are meeting an external, a DBS checked O18 staff member or volunteer should also be present for the meeting (online or in person).

7. During an online meeting/event

- Photos - do not take screenshots without parent/guardian permission (where relevant) and verbal permission from those in attendance. If you do have permission, give warning that you are going to screenshot and give everyone the chance to turn off their camera.
- Over 18s should consider blurring their background or make sure background is plain and doesn't have any personal info on display, or anything inappropriate- e.g. sweary art, drying underwear, etc.
- Use waiting room function- only the host can admit people. Don't admit anyone to the meeting until there is more than one person waiting. Do not be alone with only one U18 unless it is necessary i.e. for the purpose of the regular manager/report 1-2-1 meeting, or to discuss a specific issue.
- If anyone external gains virtual access to a private meeting, the host should remove them immediately and inform safeguarding lead.
- Keep a register of attendees and when everyone is present, lock the meeting.
- Any inappropriate or concerning comments or questions should be referred to safeguarding lead- take a screenshot of the chatbox or write down what happened.
- If an emergency happens during an online session, reassure attendees that they can leave the session. If their wellbeing or safety is at risk, call 999 if appropriate and contact safeguarding lead.
- Staff should use organisational devices rather than personal devices where possible, if staff use a personal device let the safeguarding team know.

8. Using email:

- Core staff should make it clear there's no expectation for staff or volunteers to reply outside of their agreed working/volunteering time.
- When emailing a group, use the BCC function and don't share contact details without consent.
- Find a way to make emails an 'open environment' either by cc'ing a colleague/parent or by storing the emails in an accessible place.
- Core staff should not put their personal number in their email signature. If a personal phone is used for work purposes, make sure this is logged with the safeguarding lead.
- Staff and volunteers under 18 should use a joint email account rather than individual account for emailing external organisations wherever possible.

9. Photography and video

- Staff and volunteers should always ask for written parental/guardian and the U18's consent before taking and using an U18's image. The consent request should explain what images will be used for and how they will be stored. It should also make clear that if a young person or their family withdraw consent for an image to be shared, it will be taken off all sites controlled by SOS-UK but may not be possible to delete images that have already been shared or published in places for which SOS-UK don't have full control, EG in external publications.

- For U18s who cannot gain parental/guardian consent, the safeguarding lead may make alternative arrangements, but upmost consideration will be made of whether having a photo in a public sphere is a good idea for them in their individual circumstances i.e. if parent/guardian consent is not available, does it put the young person at risk by having their photo in a public space?

Policy implementation date: 12 August 2021

Last review date: 12 August 2021