

E-Safety Policy

Online safety rules for everyone taking part in a Startup Sherpas programme.

1. Purpose and scope

Startup Sherpas runs online work experience programmes for young people aged 13-18. We are committed to providing a safe, professional and respectful digital environment. This policy explains the online spaces we use, the rules everyone must follow, the safety controls we have in place, and what to do if something goes wrong.

This policy is for everyone taking part in a Startup Sherpas programme. It covers our online platforms, live sessions and programme communications. We also have a Safeguarding Policy, which explains what our Staff must do if they are worried about the safety or wellbeing of a young person.

2. Who we mean

Participants	Young people taking part in our programmes. This includes Squad Members and Squad Leaders. A Squad Leader may help and encourage other people, but they do not get any extra access to people, personal information or messages. For this policy, they are still a Participant.
Staff	Startup Sherpas employees and paid interns. All Staff who work with Participants are appropriately DBS checked. Staff can contact Participants directly when they need to as part of their job.

3. Our online environment

Think of a Startup Sherpas programme as an online place of work. We expect everyone to be respectful, professional and safe, just as they would be in a workplace. To take part in the programme, you must follow these rules.

Startup Sherpas platform

Our Startup Sherpas platform is where you find your programme instructions, activities and information, and upload your work. You sign in to your own account. There is no social or messaging area, so Participants cannot contact each other through the platform.

Mattermost

We use our own Mattermost service for programme chat. Participants are put into programme Teams, with different channels for different activities.

- Chats take place in shared channels. Staff can see all conversations and at least one member of Staff is part of the Team/channel environment.
- Direct messages between Participants are blocked by our technology.
- Direct messages can only be sent by Staff to Participants.
- Do not try to get around this or move to messaging through other apps and platforms.
- The same rules apply to everything you post in Mattermost, including messages, links, files, images and videos.

Live video sessions

We may use Zoom, Microsoft Teams or Google Meet for live sessions. These sessions are part of the programme, so behave as you would in a supervised workplace.

- Join using the name or identity agreed for the programme. Do not pretend to be someone else.
- Dress appropriately and join from a suitable place. Where possible, use a shared or neutral space rather than a bedroom.
- Make use of the 'blur background' setting when available.
- Check what other people can see or hear in the background. Do not show personal or private information.
- Do not take screenshots, photos, audio recordings or video recordings of a session or another Participant unless Startup Sherpas has clearly said you can.
- Do not share meeting links, passwords or access details with anyone who should not be there.
- Follow instructions from Staff. For example, you may be asked to mute yourself, stop sharing your screen, remove something you have posted or leave a session.
- Startup Sherpas will not record live sessions or take photos for programme use unless the right permission has been given.

A simple rule

If you would not say it, show it or share it at school or in a place of work, do not post or send it as part of a Startup Sherpas programme.

4. Online safety risks

There are four main types of online safety risk. They are useful to know because online risks can happen on many different apps and platforms.

Content: things you see, watch or read online that are illegal, inappropriate or harmful. This could include sexual content, racism, misogyny, antisemitism, extreme violence, self-harm or suicide content, extremism, or false and misleading information.

Contact: harmful or unsafe contact with other people online. This could include peer pressure, grooming, exploitation, scams or an adult pretending to be a child or young person.

Conduct: things someone does online that could harm themselves or someone else. This includes bullying, harassment, discrimination, sharing private information, or creating or sharing sexual or harmful images.

Commerce / contract: risks involving money or online services, such as gambling, inappropriate adverts, phishing, fraud and scams.

5. Online behaviour: mandatory rules

These rules are a condition of taking part in a Startup Sherpas programme. They apply to Mattermost, live video sessions and anything else you do online as part of the programme.

- Treat Participants and Staff with respect. Do not bully, harass, threaten, intimidate, discriminate against or deliberately embarrass anyone. Sexual comments are also not allowed.
- Do not create, upload, post or share anything that is offensive, threatening, discriminatory, sexually explicit, illegal or otherwise inappropriate.
- Do not post or share photos, videos, audio or other media of another person without permission.
- Do not give another Participant your personal contact details. This includes your personal email, mobile number, home address, social media username, gaming username or anything else they could use to contact you privately.
- Do not ask another Participant for their personal contact details.
- Do not add, follow or privately contact other Participants on social media, messaging apps, gaming platforms or other personal services because you met them through the programme.
- Keep programme conversations on the Startup Sherpas platforms we provide. Do not try to get around the block on direct messages between Participants.
- Do not arrange to meet another Participant outside the programme because you met them through the programme.
- Keep your password and sign-in details private. Do not share your account or let someone else use it.
- Do not share programme meeting links, channel access, private programme information or programme content with people who should not have it.
- Do not post harmful links, viruses or malware, scams, deliberately misleading content, or anything designed to get around our safety controls.
- If you see or receive anything that makes you or someone else feel unsafe, uncomfortable or worried, tell a member of Startup Sherpas Staff as soon as you can. Do not try to investigate it yourself or share the content with other people.

Breaches of these rules

Inappropriate posts or media, cyberbullying, harassment, trying to contact Participants privately, sharing personal contact details, or other serious rule-breaking will result in immediate removal from the programme. If we think someone may be at risk of harm, abuse or exploitation, we will also follow our Safeguarding Policy. We may need to keep relevant information and pass the concern to the right safeguarding organisation or public authority.

6. Cyberbullying and harmful peer behaviour

Cyberbullying means using technology to hurt, embarrass, frighten, exclude or upset someone. It can happen more than once, but one serious message, post, image or video can also cause real harm.

- Do not reply to, forward, repost or share abusive or embarrassing content.
- Tell a member of Startup Sherpas Staff as soon as you can. If possible, leave the content where it is so Staff can deal with it properly. Do not share it with other people.
- Staff will deal with the issue using this policy and our Safeguarding Policy. Cyberbullying or harmful behaviour towards another Participant will result in immediate removal from the programme.
- If needed, Startup Sherpas may contact a parent or carer, the organisation running or funding the programme, a school or college, a safeguarding lead, the police or children's social care.

7. Sexual images, online sexual abuse and exploitation

If you are worried about sexual images or messages, grooming, pressure to do something sexual, exploitation, or an adult trying to make inappropriate contact with a Participant, tell Startup Sherpas Staff immediately. We will treat this as a safeguarding concern.

If you are a Participant

- Do not ask for, create, send, forward, save or share nude or semi-nude images or sexual content.
- If someone sends you a sexual image or message, do not forward it or show it to other people. Tell a member of Staff or another trusted adult.
- If you are worried that a sexual image or video of you has been shared online, you can also use Childline and the Internet Watch Foundation's Report Remove service.

If you are a member of Staff

- Tell the Designated Safeguarding Lead (DSL), or the person carrying out that role, straight away and follow the Safeguarding Policy.
- Do not view, copy, print, share, store or save nude or semi-nude images. Do not ask a Participant to share or download them.

- If you see an image by accident, tell the DSL, or the person carrying out that role, straight away.
- Do not ask the Participant to delete the image and do not investigate the situation yourself.
- Do not blame or shame anyone involved. Explain that you need to tell the right safeguarding person so they can help and support them.

8. Reporting a concern

If anything online makes you feel unsafe, uncomfortable or worried, tell a member of Startup Sherpas Staff. This could be something you have seen or received, another Participant's behaviour, unwanted contact, bullying, sexual content, threats, scams or someone asking for personal information.

1. Tell a member of Startup Sherpas Staff as soon as you can.
2. Do not forward, repost or share the content with other people.
3. If someone is in immediate danger or at risk of serious harm, call 999.
4. If it is a safeguarding concern, Startup Sherpas Staff will follow our Safeguarding Policy. This may include telling the DSL and, where needed, other organisations that can help keep someone safe.

9. External reporting and support

CEOP: Young people and adults can report concerns about online sexual abuse or grooming through the National Crime Agency's CEOP Safety Centre. [CEOP Safety Centre](#). We provide a link to this in the footer of every page on our Platform.

Internet Watch Foundation (IWF): Reports of child sexual abuse imagery online can be made to the IWF. [IWF reporting](#)

Report Remove: Young people under 18 in the UK can use the Childline/IWF Report Remove service to report sexual images or videos of themselves and seek removal. [Report Remove](#)

Childline: Free confidential support for children and young people is available on 0800 1111 and online. [Childline](#)

NSPCC Helpline: Adults concerned about a child can contact the NSPCC on 0808 800 5000. [NSPCC Helpline](#)

10. Responsibilities of Startup Sherpas

Startup Sherpas will take sensible steps to keep the online programme environment safe. We will:

- use approved programme platforms and safety controls;
- block direct messages between Participants in Mattermost;
- keep programme chats in shared channels that Staff can see;
- explain the behaviour rules clearly when Participants join a programme;
- make sure all Staff are appropriately DBS checked and know how to report safeguarding concerns;
- respond quickly when harmful or inappropriate behaviour is reported; and

- review our online safety arrangements if the technology we use or the way we run programmes changes.

POLICY OWNER**Helen Roe****LAST REVIEWED****September 2026****NEXT REVIEW****September 2027**