STARTUP
SHERPAS.

ESafety Policy

As a basic necessity we all want to feel safe so we ask everyone to respect these guidelines whilst taking part in a Sherpee Session.

A Sherpee Session involves a live video conference call which will take place between the Head Sherpas and Sherpees. They will use Zoom to do this. All communication are via our own platform 'Mattermost'. All of those involved will follow the guidance below:

- All participants are appropriately dressed from top to toe!
- Consideration will be given to location. An 'open' area of your home (for example kitchen, living room etc) is best rather than a bedroom.
- In terms of GDPR, be careful what is behind you when you are in a session.
- A responsible adult should monitor the Sherpee's participation whilst in a session. If Sherpees are inappropriately dressed or working in an inappropriate place, i.e. their bedroom, parents/careers will be informed and the call may be discontinued.
- All of our Community Sherpas have been DBS checked.
- The Sherpee Sessions will not be recorded or photographs taken without permission sought from parents.

Safeguarding and Online Safety

The issues classified within online safety are considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group

Online behaviours

.

- Sherpas must not create, store, transmit or cause to be transmitted material which is offensive, obscene, indecent or defamatory or which infringes the copyright of another person.

- Sherpas are discouraged from moving their online chat to another platform (eg Snapchat et) where their conversations cannot be monitored by Startup Sherpas through their platform 'Mattermost'.

- Sherpas must immediately tell 'Lama Bot' if they receive an offensive message.

- Sherpas are advised not to reveal personal details about themselves or others in e-mail communication or Teams message, or arrange to meet anyone without specific permission.

Cyberbullying

1. Cyberbullying is defined as the use of ICT to deliberately hurt or upset someone. Unlike traditional physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

2. Cyberbullying is extremely prevalent as children who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous. In extreme cases, cyberbullying could be a criminal offence.

3. Cyberbullying may take the form of:
    - rude, abusive or threatening messages via email or text
    - posting insulting, derogatory or defamatory statements on blogs or social networking sites
    - setting up websites that specifically target the victim

    - making or sharing derogatory or embarrassing videos of someone via mobile phone or email
4. Most incidents of cyberbullying will not necessarily reach significant harm thresholds and will probably be best dealt with the service's own anti-bullying or acceptable use policies with the co-operation of parents.

5. In terms of Cyberbullying, sherpees are encouraged:
    - not to disclose their password to anyone
    - not to post or respond to offensive messages
    - to tell a responsible adult about any incidents immediately.

Reporting online child abuse images

It's against the law to produce or share images of child abuse, even if the image was self-created. This includes sharing images and videos over social media.

If you see a video or image that shows a child being abused:

- Don't comment, like or share the video or image, as this will distribute it further.
- Report it to the website you've seen it on.
- Report it to the police.
- Contact the NSPCC helpline on **0808 800 5000** and we'll report it to the police for you.

If the image or video involves the sexual abuse of a child, report it to the Internet Watch Foundation (IWF) who will take steps to get it removed from the internet.

Young people under 18 who are worried that a sexual image or video of them may have been shared online can use Childline and IWF's Report Remove tool to see if it can be taken down.

Inappropriate contacts and non-contact sexual abuse

1. Children may also be sexually abused online through video messaging such as Zoom. In these cases, perpetrators persuade the child concerned to carry out sexual acts while the perpetrator watches/records them. The perpetrators may be adults but may also be peers.

2. Concerns may be raised about a child being at risk of sexual abuse as a consequence of their contact with an adult they have met over the internet. If

reported to Startup Sherpas, parents are advised to be vigilant of their child's internet use and report any concerns or incidents.

3. In the event of such an incident, the child can use the CEOP "Report abuse" button (normally displayed on the screen) and parents should contact the police to report the incident.

4. Startup Sherpas staff and parents should contact Surrey Children's Services on (0300) 123 1620 (or if outside working hours, the emergency duty team on (01483) 517898) for advice on making a referral where there are concerns that the child:
    - is being groomed for sexual abuse
    - is planning or has arranged to meet with someone they have met on-line
    - has already been involved in making or viewing abusive images
    - has been the victim of non-contact sexual abuse.

5. If Startup Sherpas staff or parents are aware that a child is about to meet an adult they have made contact with on the internet, they should contact the police on 999 immediately.

Online Child Sexual Exploitation (CSE)

1. CSE describes situations where a young person takes part in sexual activity either under duress or in return for goods, food or accommodation. A key element of CSE is that there is a power imbalance in the relationship, for example often the perpetrator is much older than the child, who may not aware that they are being abused.

2. Staff should be aware that children can be sexually exploited online, for example posting explicit images of themselves in exchange for money or goods.

3. If staff are concerned that a child they work with is being sexually exploited online, they should inform the Designated Safeguarding Lead immediately, who may make a multi-agency referral.

4. In cases where there is an online element such as sexting, specific advice must be followed:
    - **Never** view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal**.
    - If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.
    - **Do not** delete the imagery or ask the young person to delete it.
    - **Do not** ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
    - **Do not** share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
    - **Do not** say or do anything to blame or shame any young people involved.

- **Do** explain to them that you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

Online privacy and safety- resources for parents

We do our best to promote a safe and trusted community. Ultimately it is up to parents to provide education and oversight for Internet use in their homes.

Here are some resources that are good starting points:

CEOP is a website run by the police and offers a reporting function as well as more information about Online Safety.

ThinkUKnow to play interactive games with your children and learn more about being safe online.

Kidsmart has lots of information regarding safety for children and adults, it also provides information on how to avoid breaking the law through online activity.

ParentInfo has a range of information on how to support children in staying safe whilst using technology.

Brook shares support on a range of online safety issues.
Vodaphone digital parenting offers guides for parents & carers to help keep young people safe online.

ReviewLab has a good online safety guide for parents and explains some of the more technical terminology.

Childnet have some fantastic resources to aid you when talking to young people about their use of the internet from questions to ask to examples of family online safety agreements.

TigerMobiles has really handy help sheets for parents and carers with a focus on smartphones and commonly used apps.

Policy written by: H. Roe January 2024

Policy Review: January 2025