SIDEMISSION SOCIAL

ONLINE SAFETY & ACCEPTABLE USE POLICY

SIDEMISSION SOCIAL

Document owner: David Robinette and Elaine Bell

Applies to: Directors, employees, volunteers, sessional workers, contractors and participants using Side Mission Social equipment, accounts, networks or digital platforms

Review frequency: Annually, or following a significant incident or change in activities

Purpose

Side Mission Social uses digital technology as an important part of its activities and programmes.

This includes computers, laptops, mobile devices, gaming equipment, VR, music production, social media, websites, online collaboration, digital design and other creative technology.

This policy sets out how digital technology should be used safely, responsibly and respectfully.

Our approach

Side Mission Social wants young people to develop confidence and practical digital skills while understanding how to manage online risks.

We recognise that online safety is part of safeguarding.

Staff must take appropriate action where online activity creates a safeguarding concern, including concerns involving bullying, exploitation, inappropriate contact, sexual content, threats, harassment or abuse.

Acceptable use

Participants using Side Mission Social equipment, accounts or digital services are expected to:

- Use equipment and accounts responsibly.
- Follow reasonable instructions from staff.
- Respect other people's privacy and personal information.
- Use appropriate language and behaviour.
- Respect copyright and intellectual property.
- Use websites, software and online services for appropriate purposes.
- Take care when downloading files or installing software.
- Report suspicious, harmful or inappropriate content to a member of staff.
- Look after equipment and report damage or faults.
- Log out of accounts when finished.

Unacceptable use

Users must not:

- Access, create, download or share illegal or deliberately harmful material.
- Use technology to bully, threaten, harass or intimidate another person.
- Attempt to access another person's account, files or private information.
- Share passwords or deliberately bypass security controls.
- Install unauthorised software or alter security settings without permission.
- Attempt to damage, disrupt or interfere with Side Mission Social equipment, networks or systems.
- Use technology to impersonate another person or create misleading content intended to cause harm.
- Record, photograph or share another participant without appropriate permission.
- Use Side Mission Social equipment to conduct scams, fraud or other illegal activity.
- Access sexual, extremist or otherwise seriously inappropriate material using organisational equipment or services.

This list is not exhaustive. Staff may restrict access to any activity where there is a reasonable safety, safeguarding or security concern.

Personal devices

Participants may use personal devices during activities where this has been agreed by the session leader.

The same expectations around respectful behaviour, privacy, recording and online safety apply.

Staff may restrict personal device use where it is interfering with an activity, creating a safeguarding concern or presenting a risk to another participant.

Staff should not routinely access personal devices or private accounts belonging to participants.

Social media and online communication

Side Mission Social may use social media and online platforms to promote activities, share appropriate project work and communicate organisational information.

Staff must maintain professional boundaries when communicating with participants.

Where direct communication with participants is required, staff should use approved organisational channels rather than personal accounts wherever reasonably possible.

Staff must not use private or disappearing-message communication to avoid appropriate organisational oversight.

Participants should not be encouraged to provide unnecessary personal contact details to staff.

Any concerning online communication involving a participant must be reported through the safeguarding procedure where appropriate.

Photography, video and recording

Photography, video and audio recording must be carried out in accordance with the organisation's Photography and Media Consent arrangements.

Participants must not record or photograph other participants without appropriate permission.

Staff must not use personal devices to create or store participant images where an approved organisational device or process is available.

Images or recordings must only be used for the purpose for which appropriate permission has been obtained.

Any inappropriate recording, sharing or distribution of images must be treated seriously and may constitute a safeguarding concern.

Privacy and personal information

Participants must not share another person's personal information without permission.

This includes:

- Names where inappropriate to share.
- Addresses and locations.
- Telephone numbers.
- Email addresses.
- Passwords.
- Private messages.
- Personal photographs or videos.
- Information about someone's family, health or circumstances.

Staff must only collect and use participant information that is necessary for legitimate organisational purposes.

Personal information must be stored securely and handled in accordance with applicable data protection requirements.

Passwords and account security

Passwords must be kept private and must not be shared with other participants.

Staff responsible for organisational accounts should use strong, unique passwords and appropriate additional security measures where available.

Where multi-factor authentication is available for important organisational accounts, it should be enabled where reasonably practicable.

Staff must report suspected account compromise, lost devices or unauthorised access promptly.

Gaming, VR and online communities

Gaming, VR and online communities may form part of Side Mission Social activities.

Staff must consider the age rating, content, communication features and online interactions associated with games or platforms before using them with participants.

Voice chat and messaging features must be appropriately managed.

Participants must not be encouraged to communicate privately with unknown adults through organisational activities.

Staff should intervene where online interactions become abusive, threatening, sexualised or otherwise unsafe.

Music, media and creative content

Participants may use digital tools to create music, graphics, video, websites and other creative work.

Staff should encourage responsible use of copyrighted material, licensed software, images, music and other content.

Participants should be encouraged to credit sources and understand the difference between inspiration, permitted use and copying.

Content created through SMS activities must not be used to harass, threaten, discriminate against or deliberately harm another person.

Artificial intelligence and emerging technology

Side Mission Social recognises that artificial intelligence and other emerging technologies may form part of creative and educational activities.

Participants may use AI tools where appropriate and where permitted by the activity leader.

Personal, confidential or sensitive information must not be entered into AI tools unless the organisation has established that this is appropriate and lawful.

AI-generated content must not be used to impersonate, threaten, exploit, bully or deceive another person.

Where appropriate, participants should be encouraged to understand that AI-generated information can be inaccurate and should be checked before being relied upon.

Online safeguarding concerns

Any concern that a participant may be at risk online must be reported to the designated safeguarding lead (DSL) in accordance with the Safeguarding and Child Protection Policy.

This may include:

- Online bullying or harassment.
- Threats or intimidation.
- Sexual exploitation or grooming.
- Inappropriate sexual communication or imagery.
- Coercion or blackmail.
- Contact from an unknown adult presenting a safeguarding concern.
- Sharing of intimate images without consent.
- Radicalisation or extremist content.
- Self-harm or suicide-related concerns.
- Fraud, exploitation or other criminal activity.

Staff must not investigate potentially criminal or safeguarding material themselves. Relevant information should be preserved where appropriate and passed to the DSL or relevant authority.

Monitoring and supervision

Side Mission Social may use reasonable supervision and technical controls to maintain safety when participants are using organisational equipment or services.

Any monitoring will be proportionate and undertaken for legitimate safeguarding, security or operational purposes.

Staff should not assume that organisational equipment or accounts are private.

Participants will be informed about relevant rules and expectations before using organisational equipment or digital services.

Online incidents

Where an online incident occurs, staff must:

1. Take immediate steps to protect anyone at risk.
2. Inform the session leader or DSL where appropriate.
3. Preserve relevant information where safe and appropriate.
4. Avoid forwarding or distributing harmful material unnecessarily.
5. Record the incident factually.
6. Follow safeguarding, behaviour or incident procedures as appropriate.
7. Contact the police or other relevant authority where the circumstances require it.

Where an account, device or system may have been compromised, access should be restricted and the issue reported to the person responsible for organisational IT or accounts.

Staff responsibilities

Staff and volunteers must model appropriate digital behaviour.

They must maintain professional boundaries, protect confidential information and report safeguarding concerns.

Staff must not use their position to obtain inappropriate access to participants' personal accounts, devices or online activity.

Any use of organisational systems must comply with relevant policies and organisational instructions.

Consequences of misuse

Side Mission Social may restrict or remove access to equipment, accounts or digital services where someone breaches this policy.

Serious or repeated misuse may result in further action under the Behaviour and Anti-Bullying Policy, Staff/Volunteer Code of Conduct or relevant organisational procedures.

Where behaviour may involve criminal activity or a safeguarding concern, appropriate external agencies may be contacted.

Review

This policy will be reviewed annually and following a significant online safety incident, major change in technology or relevant change in guidance.

Approved By: _____ Date: _____

Signature: _____ Review Date: _____