



Acceptable Use of Technology, Mobile Devices and Social Media Policy

Policy Statement

In-Spire Sounds CIC recognises that technology, mobile devices, internet access, and social media can provide valuable opportunities for learning, communication, participation, and engagement. We are committed to promoting the safe, responsible, and respectful use of technology by all young people, staff, volunteers, and visitors.

This policy aims to:

- Promote safe and positive use of technology.
- Protect young people from harm, abuse, exploitation, and online risks.
- Maintain professional boundaries between staff and young people.
- Ensure compliance with safeguarding, data protection, and confidentiality requirements.
- Provide clear expectations regarding the use of digital technologies and social media.

Scope

This policy applies to:

- All staff, volunteers, trustees, contractors, and sessional workers.
- All young people participating in activities delivered by [Organisation Name].
- Any technology used during project activities, whether owned by the organisation or personally owned.

Principles

Everyone using technology within the project should:

- Treat others with respect and dignity.
- Use technology safely and responsibly.
- Protect personal and confidential information.
- Report concerns, inappropriate behaviour, or safeguarding issues.
- Follow applicable laws and organisational policies.



Acceptable Use of Technology

Users may:

- Access approved online resources for educational, recreational, or project-related purposes.
- Use communication platforms authorised by the organisation.
- Participate in online activities, meetings, and events arranged by the organisation.
- Access project information and resources provided by staff.

Users must:

- Follow staff instructions regarding technology use.
- Respect the privacy and rights of others.
- Use technology in a manner that supports a safe and inclusive environment.
- Obtain permission before recording, photographing, or filming others.

Unacceptable Use

The following behaviour is not permitted:

- Accessing, creating, storing, or sharing inappropriate, offensive, discriminatory, sexual, violent, extremist, or illegal content.
- Cyberbullying, harassment, intimidation, trolling, or threatening behaviour.
- Sharing personal information about others without consent.
- Attempting to bypass security systems or access unauthorised accounts.
- Downloading software, applications, or files without permission on organisation-owned devices.
- Using technology to facilitate illegal activity.
- Deliberately damaging equipment or networks.
- Recording or photographing individuals without their knowledge or permission.



Mobile Device Use

Young People

Young people may use personal mobile devices during agreed times and in accordance with project rules.

Young people must not:

- Use devices to bully, harass, or intimidate others.
- Share inappropriate images, videos, or messages.
- Photograph or record others without consent.
- Use devices in areas where privacy is expected.

Staff and Volunteers

Staff and volunteers should:

- Use organisation-issued devices where available.
- Keep personal and professional communications separate.
- Ensure personal devices used for work are protected with passwords or biometric security.
- Store and process personal information securely.

Staff and volunteers must not:

- Share personal phone numbers unless authorised.
- Use personal messaging services with young people unless approved by management and recorded as part of organisational procedures.
- Store unnecessary personal information relating to young people on personal devices.

Online Communication with Young People

All communication with young people should:

- Be professional, transparent, and appropriate.
- Take place through approved organisational channels wherever possible.
- Be related to project activities and support.
- Be capable of review by managers if required.

Staff and volunteers must not:

- Engage in secretive communications with young people.
- Use disappearing-message functions for project communications.
- Communicate with young people outside agreed project purposes.
- Develop personal online relationships with young people involved in the project.



Social Media Use

Organisational Social Media

Official organisational social media accounts may be used to:

- Promote activities and events.
- Share information and opportunities.
- Celebrate achievements.
- Engage positively with the community.

Content must:

- Reflect the organisation's values.
- Be respectful and inclusive.
- Protect confidentiality and privacy.
- Comply with safeguarding requirements.

Staff and Volunteer Personal Social Media

Staff and volunteers should:

- Maintain professional boundaries online.
- Consider privacy settings on personal accounts.
- Avoid content that could damage the reputation of the organisation or compromise professional relationships.

Staff and volunteers must not:

- Accept friend or follow requests from young people on personal social media accounts unless explicitly authorised as part of their role and approved by management.
- Share confidential information about young people, families, colleagues, or the organisation.
- Post content that could be considered discriminatory, abusive, or inappropriate.

Young People's Social Media Use

Young people are expected to:

- Use social media respectfully and responsibly.
- Treat others with kindness and respect.
- Report bullying, harassment, or concerning content to staff.
- Respect the privacy of other participants.



Photography, Video and Live Streaming

Photos, videos, and recordings may only be taken in accordance with the organisation's consent procedures.

All users must:

- Respect individual consent preferences.
- Use images only for authorised purposes.
- Store and share images securely.

Live streaming of activities is only permitted where authorised by the organisation and appropriate consent has been obtained.

Safeguarding and Online Safety

Any concerns regarding:

- Cyberbullying.
- Online grooming.
- Sexual exploitation.
- Harmful content.
- Radicalisation or extremist content.
- Self-harm or suicide-related content.
- Online abuse.

must be reported immediately to the Designated Safeguarding Lead (DSL) or appropriate manager.

Safeguarding concerns will be managed in line with the organisation's safeguarding policy and procedures.

Data Protection and Confidentiality

All users must:

- Handle personal information in accordance with data protection legislation.
- Keep passwords secure and confidential.
- Report data breaches immediately.
- Avoid sharing personal information through unsecured channels.

Confidential information relating to young people, staff, or families must not be shared on social media or through unauthorised communication channels.



Monitoring and Compliance

The organisation reserves the right to monitor the use of organisational technology, systems, and accounts where lawful and appropriate.

Failure to comply with this policy may result in:

- Removal of access to technology or systems.
- Behaviour management procedures for young people.
- Disciplinary action for staff and volunteers.
- Referral to external agencies where required.

Reporting Concerns

Any individual who becomes aware of inappropriate use of technology or social media should report their concerns immediately to:

- Project Manager
- Designated Safeguarding Lead
- Senior Manager

Reports will be treated seriously and managed in accordance with safeguarding, disciplinary, and data protection procedures.

Policy Review

This policy will be reviewed annually or sooner if changes in legislation, technology, safeguarding guidance, or organisational practice require it.

Approved By: __Kingsley Pratt Boyden____

Approval Date: ____25/10/2025____

Review Date: ____25/10/2026____