SEIN E-Safety Policy and Strategy

1. Purpose and Scope

The purpose of this policy is to:

- Safeguard all learners, staff, and stakeholders when using digital technologies.
- Promote the safe and responsible use of information and communication technologies (ICT).
- Protect the data, wellbeing, and professional integrity of all individuals connected to SEIN CIC.

Scope:
This policy applies to all online and offline activity involving SEIN CIC, including use of emails, social media, learning platforms, mobile devices, and remote learning.

2. Aims

SEIN CIC aims to:

- Educate staff, learners, and families about the risks and responsibilities of online behaviour.
- Provide clear procedures for responding to incidents and concerns.
- Ensure systems are secure, appropriate, and monitored for misuse.
- Promote a safe digital environment through proactive strategy and staff training.

3. Roles and Responsibilities

Management

- Ensure policies are up-to-date and meet national guidance (including KCSiE and Prevent Duty).
- Provide staff with training on E-safety annually.
- Appoint an E-Safety Lead to oversee implementation and respond to incidents.

Staff

- Model good online behaviour and educate learners about digital safety.
- Report any E-safety concerns or breaches immediately.
- Follow the ICT Acceptable Use Policy and maintain professional boundaries online.

Learners

- Use technology responsibly and respectfully.
- Report inappropriate or upsetting online content to a trusted adult immediately.
- Understand and follow SEIN CIC's E-safety ground rules.

Parents/Carers

- Support SEIN CIC's policies at home.
- Encourage responsible internet use.
- Report any concerns about online risks to SEIN CIC.

4. Key Principles

- **Education First**: E-safety is taught regularly through activities, workshops, and embedded in curriculum delivery.
- **Monitoring and Filtering**: All SEIN CIC technology is filtered and monitored where possible. Online activity during sessions is supervised.
- **Safe Communication**: Staff communicate with learners via authorised channels (e.g., SEIN CIC email, learning platforms).
- **Secure Systems**: Devices, platforms, and data systems are password-protected and comply with UK GDPR.
- **Confidentiality and Privacy**: Sensitive information and learner identities are protected in digital spaces.

5. Acceptable Use Rules

For Staff and Learners:

- Only use SEIN CIC approved systems for work/learning.
- Do not share personal information.
- Respect copyright and intellectual property laws.
- Never engage in cyberbullying, harassment, or inappropriate communications.
- Report concerns about online behaviour or security breaches.

6. Training and Education

- All staff will complete annual E-safety training.
- Learners will be educated about online risks such as cyberbullying, grooming, phishing, fake news, and online radicalisation.

- Parents will receive guidance materials to help support online safety at home.

7. Reporting and Responding to Incidents

If an online safety concern arises:

- Report immediately to the Designated Safeguarding Lead (DSL) or E-Safety Lead.
- The concern will be recorded following SEIN CIC's Safeguarding Procedures.
- Serious incidents (e.g., grooming, exploitation, illegal content) will be referred to external agencies (e.g., Police, CEOP).

8. Social Media Use

- Staff must maintain professional boundaries on social media.
- Learners are advised not to share personal information online.
- Staff are prohibited from accepting friend/follow requests from learners on personal accounts.

9. Online Learning

When delivering online education:

- Staff must use professional accounts only.
- Virtual sessions must follow SEIN CIC's safeguarding protocols (e.g., appropriate backgrounds, secure links).
- Online classes may be monitored for quality and safeguarding.

10. Monitoring and Evaluation

- E-safety procedures will be reviewed annually.
- Incident logs will be maintained securely and reviewed to inform practice.
- Surveys and feedback will be used to adapt the policy as needed.

SEIN E-SAFETY STRATEGY

Our strategy focuses on three core elements:

1. **Prevention**: Building resilience in learners through education and awareness.
2. **Protection**: Ensuring the technical infrastructure supports safe use.
3. **Partnership**: Working with learners, parents, and outside agencies to promote a culture of e-safety


SEN