PERSON RESPONSIBLE FOR POLICY:	***PAUL MILLS***
APPROVED:	***MICHELLE HARVEY***
SIGNED:	***PAUL MILLS***
TO BE REVIEWED:	***SEPTEMBER 2027***

UKPRN: 10101682 | Legal Address: Thistledown Barn, 204 Holcot Lane, Sywell NN6 0BG

SNAP Online Safety & Cyber Security Policy

1. Purpose

SNAP is committed to keeping learners, staff, visitors, systems and information safe when using technology.

This policy applies to everyone using SNAP's devices, systems, networks or data, on-site or remotely.

2. Responsibilities

- **Directors:** Provide oversight and approve this policy.
- **Senior Leadership:** Implement the policy and manage risks.
- **DSL:** Manage online safeguarding concerns.
- **DPO/Data Protection Lead:** Manage data protection and data breaches.
- **IT Support:** Maintain systems, security, devices, updates and access.
- **All Users:** Follow this policy, use technology responsibly and report concerns immediately.

3. Online Safety

SNAP will teach learners how to use technology safely and responsibly, including:

- Recognising harmful content and online contact.
- Cyberbullying and inappropriate behaviour.
- Protecting personal information.
- Safe use of social media, gaming and online services.
- Knowing how and where to get help.

Online safeguarding concerns must be reported to the DSL.

Learners requiring additional support will receive appropriate help and supervision.

4. Cyber Security

SNAP will maintain appropriate security controls, including:

- Strong passwords and MFA where available.
- Appropriate user access.
- Secure and encrypted devices where supported.
- Regular updates and anti-malware protection.
- Firewalls, filtering and monitoring.
- Secure backups.
- Approved software, apps and cloud services.

Users must not share passwords or use unapproved systems to store SNAP information.

5. Data Protection

SNAP will comply with UK GDPR and the Data Protection Act 2018.

Personal and confidential information must be kept secure and only accessed or shared when necessary.

Suspected data breaches must be reported immediately. Where legally required, the ICO will be notified within 72 hours.

6. Filtering and Monitoring

SNAP will use appropriate filtering and monitoring to help protect learners from harmful or inappropriate online content.

Safeguarding alerts will be referred to the DSL.

7. AI and Online Services

Personal, confidential or sensitive information must not be entered into public AI tools or unapproved online services.

Staff are responsible for checking AI-generated information before using it.

8. Reporting Incidents

All users must immediately report:

- Phishing or scam emails.
- Lost or stolen devices.
- Unauthorised access.
- Malware or ransomware.
- Data breaches.
- Cyberbullying or online safeguarding concerns.

Incidents will be recorded, investigated and managed appropriately.

9. Compliance and Review

SNAP is not a registered school or college, so KCSIE is not directly statutory. SNAP will follow relevant safeguarding principles and applicable guidance, including *Working Together to Safeguard Children*, relevant DfE guidance, UK GDPR and the Data Protection Act 2018.

This policy will be reviewed annually and approved by Directors.