Online Safety Policy (E-Safety)

Purpose of the policy

We are committed to promoting the safe, responsible and appropriate use of digital technology by staff, associates and learners.

This policy supports our safeguarding responsibilities and aims to protect children, young people and adults at risk from online harm. It also supports our duties under safeguarding legislation, the Prevent Duty and other relevant guidance relating to online safety.

Scope of the policy

This policy applies to:

- All staff
- Associates
- Apprentices
- Learners
- Volunteers
- Anyone using our company systems, devices or online platforms.

The policy applies whether technology is used on company premises, remotely or during online learning and meetings. This policy should also be read alongside our other policies on data and security, including:

- Safeguarding and Prevent Policy
- Information Technology Use Policy
- Data Protection Policy
- Privacy Policy
- Cultural Code for Staff and Workforce
- Disciplinary Policy
- Whistleblowing Policy

These can be found on our website here.

Role and responsibilities

At Sport Structures:

- The Chief Executive Officer and Head of Commercial is responsible for reviewing this policy once a year and ensuring it is included in any staff/associate induction process and is available to all staff and associates for reference
- Line Managers are responsible for ensuring that staff understand their responsibilities and know how to report IT problems or security concerns.
- Employees and associates are responsible for reading and following this policy

Staff and associates must:

- Use technology safely, appropriately and professionally.
- Maintain professional boundaries with learners.
- Complete safeguarding, Prevent and online safety training as required.
- Follow data protection and information security requirements.
- Report concerns immediately to one of the Designated Safeguarding Leads (DSL).
- Follow company procedures when delivering online learning or communicating with learners.

Apprentices/learners are expected to:

- Use technology responsibly and respectfully.
- Protect their personal information.
- Treat others appropriately online.
- Report online safety concerns to a member of staff.
- Follow the learner code of conduct

The Designated Safeguarding Leads are responsible for:

- Managing online safety concerns and incidents.
- Providing advice and support to staff and learners.
- Making referrals where safeguarding concerns are identified.
- Monitoring trends and ensuring appropriate training is in place

Safe use of technology

We will take reasonable steps to ensure systems and platforms are secure and appropriate for business and learning purposes.

Staff must:

- Use approved systems and applications wherever possible.
- Keep passwords secure and confidential.
- Follow company data protection requirements.
- Ensure devices used for work are appropriately protected.
- Not share confidential or personal information unless authorised and secure methods are used.

Personal devices may be used for authorised business purposes where suitable security measures are in place and company policies are followed

Online learning and virtual delivery

Where online learning, meetings or assessments take place, staff must:

- Use approved platforms wherever possible.
- Apply security features such as passwords, waiting rooms and participant controls where available.
- Share joining details only with authorised participants.
- Maintain professional standards of conduct.
- Follow safeguarding procedures where concerns arise during online activity.

Learners are expected to behave appropriately during online sessions and comply with reasonable instructions issued by tutors.

Social media and professional boundaries

Staff must maintain clear professional boundaries with learners at all times.

Staff must not:

- Use personal social media accounts to communicate with learners.
- Accept or initiate personal social media connections with current learners where this could create a safeguarding risk.
- Create informal communication channels with learners outside approved methods of communication.

Communication with learners should only take place through approved company systems and for legitimate educational or business purposes.

Any concerns regarding online conduct, professional boundaries or inappropriate communication must be reported to one of the Designated Safeguarding Leads.

Artificial Intelligence

The use of AI tools must be lawful, responsible and appropriate. Staff and learners must not:

- Upload confidential, personal or sensitive information into public AI platforms without authorisation.
- Use AI-generated content without reviewing its accuracy and suitability.
- Rely solely on AI-generated information for assessment, safeguarding or decision-making purposes.

Any use of AI must comply with company data protection, safeguarding and information security requirements.

Reporting concerns

Any online safety concern should be reported immediately. Concerns may include:

- Radicalisation or extremism
- Online grooming
- Cyberbullying
- Exploitation
- Inappropriate images
- Harmful online content
- Fraud or scams
- Inappropriate communication
- Breaches of professional boundaries

All concerns will be managed in accordance with our Safeguarding and Prevent Policy and other relevant company policies.

Staff should also report low-level concerns regarding the online behaviour of colleagues where this may indicate poor professional judgement, breaches of professional boundaries or safeguarding risks.

Training and Awareness

We will ensure that staff receive appropriate Safeguarding, Prevent and online safety training relevant to their role.

Learners will be provided with online safety guidance as part of induction, onboarding or curriculum delivery where appropriate.