E-Safety Policy

Introduction

Sport Structures recognises the benefits and opportunities which new technologies offer to enhance learning. We encourage the use of technology in order to learn new skills and promote achievement. However, the accessible and global nature of the internet and the variety of technologies available mean that we are aware of potential risks and challenges associated with such use. Our approach is to implement safeguards and to support staff and learners to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies. To safeguard those we work with, we will do all that we can to make our learners and staff stay safe and to satisfy our wider duty of care. This e-safety policy should be read in conjunction with other relevant policies.

Purpose

By following this policy and receiving proper training, people representing Sport Structures:

- Be able to identify potential risks in their working environment and mitigate against these risks.
- Identify the different risks which young people and adults at risk might be exposed to through the use of technology and know the signs which might suggest a participant is in danger.
- Be able to respond appropriately to allegations and concerns.
- Understand the roles and responsibilities of other professionals and know what to do if they are concerned about the actions others have taken.

rectors at Sport Structures will:

- Monitor the implementation of this policy.

- Arrange and mandate regular training for all staff, which is appropriate to their role and responsibility.

- Ensure lessons are learnt through their own regular evaluations and feedback from other agencies.

- Respond to any concerns promptly which implicate Sport Structures or volunteers.

E-safety risks

This policy identifies the risks and details the strategies involved in minimising E-Safety risks.
Guidance on dealing with youth producing sexual imagery can be found in Appendix 1 of this policy.

Examples of E-Safety Content

- Exposure to age-inappropriate material.
- Exposure to inaccurate or misleading information.
- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance.
- Exposure to illegal material, such as images of child abuse.
- Exposure to extremist or radical views/materials.

Examples of E-Safety Contact

- Grooming using communication technologies, leading to sexual assault and/or child prostitution.
- Grooming using extremist or radical views/materials for the purpose of illegal activity.

Examples of E-Safety Commerce

- Exposure of minors to inappropriate commercial advertising.
- Exposure to online gambling services.
- Commercial and financial scams.

Examples of E-Safety Culture

- Bullying via websites, mobile phones or other forms of communication devices.
- Downloading of copyrighted materials e.g. music and films.

Policy scope

The policy applies to all members of staff and learners who have access to the Sport Structures IT systems; both on the premises and remotely. The E-Safety Policy applies to all use of the Internet and electronic communication devices such as e-mail, mobile phones, games consoles, social networking sites, and any other systems that use the Internet for connection and providing of information. It should also be read alongside the Sport Structures Data Protection Policy.

Roles and responsibilities

Safeguarding is everybody's business at Sport Structures. There are clear lines of responsibility for reporting concerns regarding safeguarding within Sport Structures. The first point of contact should be the Designated Safeguarding Lead (DSL). All staff and volunteers are responsible for ensuring the safety of learners and should report any concerns immediately as per the safeguarding procedures. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

All learners must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be the DSL. Where any report of an e-safety incident is made, all parties should know what procedure is triggered and how this will be followed up.

Where management considers it appropriate, the DSL may be asked to intervene with appropriate additional support from external agencies.

Security

Sport Structures will do all that it can to make sure the network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, workstations etc. to prevent accidental or malicious access to systems and information. Digital communications, including email and internet postings, over the network, will be monitored.

Personal electronic equipment, e.g. phones, laptops, iPads etc. must not be used to hold or transmit personal data of anyone related to the business without the express permission of a Director. Failure to adhere to this may be considered Gross Misconduct.

Password Management

All staff are expected to conduct good password hygiene including not using obvious or repeat passwords for all systems providing access to personal or confidential information.

Behaviour

Sport Structures will ensure that all users of technologies adhere to the standard of behaviour as set out in the Staff Handbook and/or Code of Conduct or in the case of the participant in the learner agreement. Sport Structures will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and volunteers should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the Sport Structures disciplinary policies and procedures.

Where conduct is found to be unacceptable Sport Structures will deal with the matter via internal disciplinary procedures as described in the staff handbook. Where conduct is considered illegal Sport Structures will report the matter to the police.

Use of images and videos

The use of images, or photographs, is an integral element of some learning programmes and should be encouraged where there is no breach of copyright or other rights of another person. This will include images downloaded from the internet and images belonging to staff or learners.

All learners and staff should be aware of the risks of downloading these images as well as posting them online and sharing them with others. There are particular risks when personal images are posted on social networking sites for example.

Personal information

Personal information is information about a particular living person. Sport Structures collects and stores the personal information of learners and staff regularly e.g.

names, dates of birth, email addresses and information regarding participation. This information is stored in accordance with the Sport Structures Data Protection Policy and the latest data protection legislation.

Staff must keep learners' personal information safe and secure at all times. When using an online platform, all personal information must be password protected. No personal information of individuals is permitted offsite unless the member of staff has the permission of their Line Manager.

All personal information must be stored on centralised systems and secured by password or encryption where possible.

Education and Training

With the current unlimited nature of internet access, it is impossible for Sport Structures to eliminate all risks for staff, volunteers and learners. It is our view, therefore, that Sport Structures should support staff, volunteers and learners through training and signposting. This will provide them with the skills to be able to identify risks independently and manage them effectively. Staff, volunteers and learners should be signposted to Internet Safety courses at the beginning of any course or as part of the departmental induction. The guidance in this E-Safety Policy should be shared with staff and learners by being accessible on the website and include a link to the UK Safer Internet Centre.
https://www.saferinternet.org.uk/advice-centre/young-people

Incident and Response

Where an e-safety incident is reported to Sport Structures this matter will be dealt with very seriously. Sport Structures will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a participant wishes to report an incident, they can do so to their tutor or the DSL. Where a member of staff wishes to report an incident, they must contact their line manager or the DSL. Following any incident, the DSL will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place; external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

Whenever in doubt, employees and volunteers should contact the DSL on the numbers below for advice and guidance.

Safety Using Online Technology

All staff must ensure they are as safe when using online technology. It is Sport Structures policy that as a first port of call, the Sport Structures LMS system should be used for online classrooms and video conferencing as well as Microsoft Teams. It may be that learners involved in meetings or lessons are unable to use the Sport Structures system or maybe more comfortable using another system such as Zoom. If using Zoom, staff have a responsibility for make these as secure as possible (i.e. through password protecting and requesting that meeting invites are not shared with anyone else other than the learner) but staff should be encouraging the use of the Sport Structures systems as this is more secure and in the control of the company.

The following safety measures should be conducted whenever an online classroom or meeting is being scheduled:

- Ensure any participants who are under 18 or vulnerable are supervised if appropriate.
- Ensure meetings are password-protected where possible.
- If the meeting is public, ensure only the host/tutor can share the screen (if possible on the software) by turning on this functionality and only authorising screen shares when they know and trust the person requesting it.
- If possible set up waiting rooms or authorisation for anyone entering the session.
- Do not share meeting details, links or passwords publicly or on social media, including in 'closed' groups, and only share them privately with attendees you know and trust.
- Host or tutor should familiarise themselves with all security functions of the software being used so they can effectively run a safe session.
- The host or tutor should encourage participants to share a camera where possible and ensure participants are suitably dressed and presented for the session as they would be required to be for any face-to-face interaction.
- Be able to identify potential risks in their working environment and mitigate against these risks.
- Identify the different risks which young people and adults at risk might be exposed to through the use of technology and know the signs which might suggest a participant is in danger.

The Designated Safeguarding Lead is
Jobeth Hamilton Jobeth.Bastable@sportstructures.com 07917 388166 Sport Structures, Suite 8, The Cloisters, 12 George Road, Edgbaston, Birmingham B15 1NP

Social Media Safety

Conduct
Staff are reminded that their professional responsibilities at Sport Structures require them to act professionally in their social networking and internet activities, and to create a clear distinction between their social and their professional lives. Contact with learners must remain within the boundaries of their professional lives and contact with students should only be made through official Sport Structures social media outlets. The guiding principle here is "think before you post."

(Please see Sport Structures Safeguarding Policy, Social Media Policy, Code of Conduct and Staff Handbook for further guidance on conduct)

Where staff make use of web-publishing and social networks for professional purposes they are expected to:

- Behave professionally and with integrity
- Adhere to Sport Structures policy guidelines
- Respect their audience
- Promote productive conversations
- Protect and enhance the value of Sport Structures' reputation
- Protect confidential and business-sensitive information
- Be personable, add value and encourage responses
- Understand the safety aspects including what is acceptable and unacceptable behaviour on social media
- Be proactive in correcting any errors made
- Reporting other breaches of terms of service

Staff and volunteers must not post comments or any other information on any public forum, website, social networking site or blog:

- That are unsubstantiated and/or negative about Sport Structures (or other organisations within the Group), their colleagues, our learners, parents, or customers.
- That run counter to Sport Structures Equality and Diversity, and Safeguarding Policies.
- That recommend or appear to endorse law breaking of any kind.
- That give an account of any inappropriate behaviour.
- Nor should such comments be made in emails sent in an official or professional capacity.

Communications between staff and current or prospective learners should only take place for legitimate, professional reasons. In some cases, there may be a non-professional reason for a relationship to exist beyond the Business. (e.g. common academic interest/common membership of a club, society or team/family members). In such circumstances social communication may occur. Staff should, however, be aware of the risks involved and use their professional judgment to ensure that this communication is limited appropriately.

A member of staff inviting a current or prospective learner to join a network without any professional purpose or inviting them to 'follow' a purely personal profile will be regarded as inappropriate and potentially subject to formal disciplinary action. The risks in this situation are clear and there can be no justification and it could be considered Gross Misconduct. Where such a situation arises Sport Structures reserves the right to demand an explanation for this action and act accordingly.

Accepting any invitation to 'friend', follow or become part of a current or a prospective learners' personal network is also considered inappropriate no matter

what platform is used. Do not create one to one communication channels via social media with learners that are under 18 or are vulnerable adults at risk.

We recognise staff may wish to take part in online communities also used by learners. In such cases staff should ensure that personal information is secured. Any staff member contributing under a personal profile is obliged to ensure that minimal personal information is visible under that profile.

Official Use
As a general principle, staff should use their Sport Structures contact details or a 'professional' profile for communication with current and prospective learners and ensure that any communication is both professional and necessary. Email contact with learners, parents and other stakeholders should be channelled through the Sport Structures email system. Staff should pay particular attention when replying to emails forwarded to a personal account as these will appear to the recipient as having been sent from the personal account. Sport Structures will continue to develop the use of social media for marketing, communications and education purposes.

To assist staff in posting factual and professionally presented information without using personal details, Sport Structures will offer coordinated guidance, support and training in the management of a professional online presence and appropriate and effective use of social networks as an educational and communication tool, if requested by staff.

Authorised Sport Structures networks (group/page/blog) which exist for a clear professional purpose should be discussed with the Senior Leadership Team who will offer advice and guidance on what is acceptable.

Staff creating or participating in authorised networks should do so either anonymously, where this is possible, or under a professional profile. A professional profile is where a member of staff maintains an online presence explicitly for professional purposes. This profile should minimise any information which could be used to compromise the individual and should not be used to record social activity or personal opinion but may be used to record professional information or opinion. It is important that a professional profile is not added to non-professional networks or linked to the profiles of others except where the connection is professional. This might legitimately include links to participant groups but would be unlikely to include groups of friends/family.

Monitoring
Under certain circumstances, Sport Structures may need to monitor staff and participant email communication and use of the internet via the Sport Structures internet link. We recommend that staff monitor their own online presence, in particular, any material posted by others about them. If staff become aware of, and/or are concerned about, any critical or unprofessional comments that are

posted by colleagues they should draw these initially to the attention of the DSL in order that an official response may be posted if appropriate.

In general, personal use of social networks is discouraged particularly where an alert service or other desktop 'widget' may interrupt workflow. Professional use should be transparent and any request to view interactions respected.

It is acknowledged that existing and new staff members may already have a significant online presence with membership in complex social networks. It is the responsibility of staff to consider their existing and ongoing online activity in line with this policy guidance.

Learner Conduct
Learners must abide by the terms of any learning agreement by respecting the rights of other learners. They should think carefully about how they express themselves, and bear in mind the need to safeguard themselves.

E-Safety Policy
Material posted on the internet can be hard to delete and should, therefore, be considered permanent.

Learners must not post comments on a social networking site or blog, or send text messages:
- That could be viewed as bullying or harassing other learners.
- That are counter to Sport Structures Equality and Diversity Policy.
- That explicitly encourages other members of the community to break the law.
- That are likely to bring Sports Structures (or other organisations within the group) into disrepute.
- Learners should not post photos that they might not wish others to see.
- Learners must not share photos that are deemed to be "youth-produced sexual imagery."

Where staff become aware of this a procedure to follow is outlined in Appendix 1 of this policy.

Learners should not invite staff to join social networks or follow purely personal profiles.

Learners in apprenticeship programmes will be given guidance on the appropriate use of the Internet and e-safety through their curriculum.

If a participant has cause for concern regarding the use of the internet or social networking, they must report the incident immediately to a member of staff. There may be occasions where this will be treated as a safeguarding issue.

Appendix 1: Guidance on Dealing with Youth-Produced Sexual Imagery

The initial review meeting should consider the initial evidence and aim to establish:
- Whether there is an immediate risk to a young person or young people.
- If a referral should be made to the police and/or children's social care.
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed.
- What further information is required to decide on the best response?
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services.
- Any relevant facts about the young people involved which would influence risk assessment.
- If there is a need to contact another organisation, school, college, setting or individual.
- Whether to contact parents or carers of the people involved - in most cases parents should be involved.

An immediate referral to police and/or children's social care should be made if at this initial stage:
- The incident involves an adult.
- There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs).
- What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage or are violent.
- The imagery involves sexual acts and any pupil in the imagery is under 18.
- You have reason to believe a learner is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming.

If none of the above applies, then Sport Structures may decide to respond to the incident without involving the police or children.

Assessing the risks
The circumstances of incidents can vary widely. If at the initial review stage, a decision has been made not to refer to police and/or children's social care, a further review (including an interview with the young people involved) should be made to establish the facts and assess the risks.
When assessing the risks, the following should be considered:
- Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
- Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
- Are there any adults involved in the sharing of imagery?