|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Assessment** | | | | |
| **Risk Assessment for the activity of** | **MMA** | | **Date** | **26/09/20** |
| **Unit/Faculty/Directorate** |  | **Assessor** |  | |
| **Line Manager/Supervisor** | ***Daniel Callaghan – Health and Safety Officer*** | **Signed off** |  | |

| ***PART A*** | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **(1) Risk identification** | | | **(2) Risk assessment** | | | | **(3) Risk management** | | | |
| **Hazard** | **Potential Consequences** | **Who might be harmed**  **(user; those nearby; those in the vicinity; members of the public)** | **Inherent** | | |  | **Residual** | | | **Further controls (use the risk hierarchy**  **)** |
| **Likelihood** | **Impact** | **Score** | **Control measures (use the risk hierarchy)** | **Likelihood** | **Impact** | **Score** |
| Security/privacy issues related to use of video or voice call software. | Data protection breach | All participants | **3** | **2** | **6** | * Create password for participants * Ask participants to verify whether they are a student/member of SUSU * Avoid publishing links and passwords on social media or in public forums * Participants to be directed not to pass on link details to persons who are not members of SUSU, regardless as to how well they know them * Non-members should only be allowed to join if they are trusted by the committee, provide a clear benefit to the society such as instruction/guidance and can be verified by the host * Meeting host to compare the list of participants within the digital platform against the list of those expected to be in attendance at the start of every meeting. | **1** | **2** | **2** | Virtual meeting host to remove uninvited participants from the meeting where possible |
| Using other person’s personal details to host or participate in public events | Data protection breach | Person whose details are used | **3** | **2** | **6** | * Students to stream and join sessions using their own software account and identity rather than using another person’s details * If a participant is using another person’s device, they should change the automatic participation name as to alert others they are using the profile of another. | **1** | **2** | **2** |  |
| Participants have remote access to other’s devices | Data protection breach | All participants | **2** | **3** | **6** | * Activity host to switch off device access in account settings to ensure others cannot alter important information. * Participants to be reminded not to give access to or request access from the activity host | **1** | **3** | **3** |  |
| Unauthorised recording of sessions | Data protection breach | All participants | **2** | **3** | **6** | * Ensure all participants are aware that the session must not be recorded by any person  unless agreed and publicised clearly beforehand and with a clear description of how the recording will be used and who it will be available to. * Recordings that are authorised should also be checked to ensure any content in the video abides by university guidelines. | **1** | **3** | **3** | * Activity hosts to make participants aware if they notice a person is recording session without prior agreement * If observed to be recording; activity hosts to ask the person to stop. Refusal justifies removal from the activity. |
| Inappropriate behaviour | Bullying and harassment of participants | All participants | **2** | **3** | **6** | **SUSU believes everyone should be able to enjoy their time at university and all the experiences that go along with that. SUSU has a zero-tolerance approach regarding discrimination, prejudice, hate crime, racism, sexual misconduct, and any vicitimisation through any activity, including online**   * Participants to be reminded to be respectful of others * Activity host to have read SUSU’s Expect Respect Policy   <https://www.susu.org/downloads/SUSU-Expect-Respect-Policy.pdf> | **1** | **3** | **3** | * Activity host to remove participants from the online activity if they are behaving inappropriately * Activity host to report inappropriate behaviour to SUSU’s Activities team (activities@susu.org) |
| **Those not signed up to register may show up to sessions or may accidentally show up to the wrong session.** | Would result in unwanted mixing of bubbles, which during COVID time currently, could be hazardous for the health of many. | * Those taking part with pre-existing health condition (asthma etc). * Elderly people. | **2** | **3** | **6** | * Ensure every society member is aware properly on how to utilise the online booking system. * Ensure every member is checked at the door to ensure they are attending the correct session they signed up for.   Do not allow attendees who have not pre-booked. | **1** | **3** | **3** | * **Email every signed up attendee before session to confirm attendance.** |
| Malware | Could result in breach of university and personal data for all participants. | * Ensure if sent a link by committee member, that the link is legitimate and the committee member is who they say they are. | **2** | **3** | **6** | * Further reinforce the importance of not sharing profiles with anyone for any reason. * Ensure all links sent to registers or external media are safe and checked. | **1** | **3** | **3** | * Advocate for common sense and basic internet safety when sharing links. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***PART B – Action Plan*** | | | | | | | |
| **Risk Assessment Action Plan** | | | | | | | |
| **Part no.** | **Action to be taken, incl. Cost** | **By whom** | **Target date** | | **Review date** | **Outcome at review date** | |
| 1 | Register for every session+ confirmation email of attendance for each person before a session. | Laura Smith | 21/09/20 | |  | Registers have been put into action for fresher’s. | |
| 2 | Prevent un-authorised recording of sessions unless consent given. | All participants | 21/09/20 | |  | Participants have been informed of the rules regarding recording during sessions. | |
| 3 | Ensure access to the attendance register is well protected and passwords are kept discreet. | Laura Smith | 21/09/20 | |  | Sharing of passwords and accounts has been restricted and strongly advised against. | |
| 4 | Session ‘bouncer’ to check every person coming into the session is on the attendance register |  | 21/09/20 | |  | Attendance registers are available to the committee to ensure sessions are appropriately attended. | |
| 5 | Enforce no sharing of email passwords or account to prevent personal data breach. | All participants | 21/09/20 | |  | Participants have been informed of the importance of privacy with regards to attendance register | |
| 6 | Activity host to keep all confidential and privacy information private unless absolutely necessary. | Laura Smith | 21/09/20 | |  |  | |
| 7 | Reinforce a friendly and tolerant environment to ensure no inappropriate behaviour is tolerated. | All participants | 21/09/20 | |  |  | |
| Responsible manager’s signature: Daniel C | | | | | Responsible manager’s signature: Laura Smith | | |
| Print name: DANIEL CALLAGHAN | | | | Date: 21/09/20 | Print name: LAURA SMITH | | Date: 21/09/20 |

**Assessment Guidance**

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Eliminate | Remove the hazard wherever possible which negates the need for further controls | If this is not possible then explain why |  |
| 1. Substitute | Replace the hazard with one less hazardous | If not possible then explain why |
| 1. Physical controls | Examples: enclosure, fume cupboard, glove box | Likely to still require admin controls as well |
| 1. Admin controls | Examples: training, supervision, signage |  |
| 1. Personal protection | Examples: respirators, safety specs, gloves | Last resort as it only protects the individual |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **LIKELIHOOD** | 5 | 5 | 10 | 15 | 20 | 25 |
| 4 | 4 | 8 | 12 | 16 | 20 |
| 3 | 3 | 6 | 9 | 12 | 15 |
| 2 | 2 | 4 | 6 | 8 | 10 |
| 1 | 1 | 2 | 3 | 4 | 5 |
|  | | 1 | 2 | 3 | 4 | 5 |
| **IMPACT** | | | | |

|  |  |  |
| --- | --- | --- |
| Impact | | Health & Safety |
| 1 | Trivial - insignificant | Very minor injuries e.g. slight bruising |
| 2 | Minor | Injuries or illness e.g. small cut or abrasion which require basic first aid treatment even in self-administered. |
| 3 | Moderate | Injuries or illness e.g. strain or sprain requiring first aid or medical support. |
| 4 | Major | Injuries or illness e.g. broken bone requiring medical support >24 hours and time off work >4 weeks. |
| 5 | Severe – extremely significant | Fatality or multiple serious injuries or illness requiring hospital admission or significant time off work. |

Risk process

1. Identify the impact and likelihood using the tables above.
2. Identify the risk rating by multiplying the Impact by the likelihood using the coloured matrix.
3. If the risk is amber or red – identify control measures to reduce the risk to as low as is reasonably practicable.
4. If the residual risk is green, additional controls are not necessary.
5. If the residual risk is amber the activity can continue but you must identify and implement further controls to reduce the risk to as low as reasonably practicable.
6. If the residual risk is red do not continue with the activity until additional controls have been implemented and the risk is reduced.
7. Control measures should follow the risk hierarchy, where appropriate as per the pyramid above.
8. The cost of implementing control measures can be taken into account but should be proportional to the risk i.e. a control to reduce low risk may not need to be carried out if the cost is high but a control to manage high risk means that even at high cost the control would be necessary.

|  |  |
| --- | --- |
| Likelihood | |
| 1 | Rare e.g. 1 in 100,000 chance or higher |
| 2 | Unlikely e.g. 1 in 10,000 chance or higher |
| 3 | Possible e.g. 1 in 1,000 chance or higher |
| 4 | Likely e.g. 1 in 100 chance or higher |
| 5 | Very Likely e.g. 1 in 10 chance or higher |