Online Safeguarding Policy

1. Introduction

Health Sciences University is committed to ensuring a safe and supportive environment exists for all staff and students engaging in online outreach and engagement activities.

This document is designed to provide Health Sciences University staff and Student Ambassadors working with children and young people online with guidance and a set of procedures to follow to ensure that they adhere to the University's policy on the Safeguarding of Children and Adults At Risk (as defined in the Care Act, 2014).

This document was written with specific reference to online activities including, but not limited to, interaction on online platforms, instant messaging/chat, live videos/webinars and mentoring.

Safeguarding concerns can take many forms including, but not limited to, bullying and cyber bullying, child sexual exploitation/trafficking, domestic abuse, emotional abuse, grooming, neglect, online abuse, physical abuse, sexual abuse. Abuse could be by adults, or by other children/young people.

This policy applies to all staff/students involved in the delivery and supervision of online work. This includes University staff members, as well as temporary workers such as student ambassadors.

The purpose of this policy is to;

1.1 Provide specific guidance for staff and students delivering online outreach and engagement activities to children and young people.
1.2 Set out the University College's approach to safeguarding children, young people and adults at risk engaging in online outreach.

The University recognises that the success of the Policy will depend on its effective implementation. It will therefore ensure the effective dissemination of this Policy within the University and will provide appropriate training for key staff and Student Ambassadors as appropriate.

2. Scope of this Policy

This policy specifically relates to online outreach and engagement activities. This policy should be read alongside AECC University College's Safeguarding Policy.

3. Areas of risk

3.1 Risk Assessment

Some key risks in online activities are highlighted below. For all new activities planned, a risk assessment should be undertaken which should be approved by the responsible officer leading the activity and reviewed by the Health and Safety Officer. This risk assessment should be shared with all members of staff involved in the online activity.

3.2 IT Safety and Data Protection (additional requirements White Paper 2019)

The below considerations are highlighted in line with the IT safety and data protection White Paper 2019

3.2.1 A privacy notice for the given activity should be provided in advance of the activity, easily accessible and provided in language that the participants can understand and are thus fairly informed.

3.2.2 Data protection best practice for any data gathered and stored should be considered in advance of the activity. Data protection should be considered at all stages of design ensuring the approach mitigates the risk to individual participants' information.

3.2.3 The appropriateness of the platform and how they store, process and use personal data should be considered in deciding on an appropriate platform for deliver of the online activity.

3.2.4 For assistance in compliance with Data Protection Regulations, please contact the Data Protection Officer (dpo@aecc.ac.uk)

3.3 Social Media

3.3.1 Staff and Student Ambassadors must not engage or communicate with children, young people or their families via personal or non-university-authorised accounts – all communications should come from an official university account

3.3.2 For all activities, online or face-to-face, consent should be sought from parents/carers and the child/young person before posting any identifiable information and/or images of children and young people on social media.

3.3.3 Concerns about social media content or posts involving children and young people such as cyberbullying, self-harm, abuse or exploitations should be raised with the designated safeguarding officer in line with the process in the overarching safeguarding policy

3.3.4 Staff and Students working on online outreach and engagement projects should abide by the general principles of the code of conduct policy, communications policy, and other relevant Health Sciences University staff policies.

3.3.5 Staff and students working on online outreach and engagement policies should not use social media in a way which would breach other university policies, including the safeguarding policy.

3.4 Live activities and streaming

The measures below are as much about protecting University staff and students leading online outreach activities, as they are about supporting children and young people engaging in these.

Live streaming is not always the best way of delivering an outreach activity. Consider the alternatives and document the reasons for choosing live streaming for the individual activity. However, it is recognised that sometimes there will be reasons for choosing a live platform, such as building a sense of community/belonging amongst a particular student group and learning together.

3.4.1 Where live streaming is deemed the best platform for delivery, ensure a risk assessment has been carried out ahead of the activity and is shared with all involved.

3.4.2 Any online activities should only be delivered via online platforms approved for use by the University.

3.4.3 Access to the individual platform should only be enabled for the intended participants. This may be in the form of a waiting room, where only named students registered for the individual session are admitted.

3.4.4 The platform should enable the presenter to control microphones/cameras for participants (in particular mute a participant or turn their camera off if necessary)

3.4.5 Contracted Health Sciences University Staff delivering activities should not use their own laptop or device to engage with young people

3.4.6 Personal accounts for platforms such as Zoom and Microsoft Teams so should not be used to engage with young people, all activities should be organised through official University accounts

3.4.7 Personal information (including names, contact details and email addresses) should only be accessible to those with the right permissions and should not be publicly viewable

3.4.8 Staff and Student Ambassadors are advised never to give out personal details to participants such as personal email address, personal phone number or social media accounts.

3.4.9 Staff facilitating activities and monitoring any enabled chat should be able to remove people from the platform if necessary.

3.4.10 For all live activities, at least two members of staff/Specialist Student Ambassador's should be present to supervise the activity. It is recommended that at least one of these have a DBS check. It is recommended there is at least one member of staff presenting and another present and monitoring any messages on the platform. If possible, there should be a third staff member or Specialist Student Ambassador available to take over in case of any technical issues.

3.4.11 During a live session, staff or students organising it should:

• Ensure that the session is taking place in a neutral area where nothing personal can be seen and there is nothing inappropriate in the background, for example, images or text which may be offensive to someone.

• Monitor interactions (verbal and in live chats) to check it is appropriate and relevant, and to deal with any offensive comments or content not in line with the published code of conduct

3.4.12 If one staff member leaves the session for any reason (e.g. connection issues), they should get in contact with the other staff member as soon as possible (by phone if necessary) and attempt to re-join the session if possible. If it is not possible to have

two members of staff present, then the event should be ended as soon as reasonably possible and this should be communicated to all participants. The only exception to this would be in a school-based session, where a teacher is present on the virtual session and can act as the second adult.

3.4.13 At the start, the main speaker should remind participants how to keep themselves safe (as outlined above) in addition to reminding them of the ground rules. This is also a good time to restate any pre-shared privacy notice to participants and particularly important if participants can override any central setting and share their own video.

3.4.14 Challenging behaviour or inappropriate comments should be dealt with immediately, which may involve muting or removing the offender from the platform

3.4.15 You should also advise that the participants:

- Do not share private information about themselves
- Do not respond to contact requests from people they do not know
- Understand who they should contact if they hear anything upsetting or inappropriate

3.4.16 For any interactive livestreaming, consent should be sought and recorded from parents/guardians of any under-16 participants. Over 16 participants are able to give consent to take part by registering for sessions. To require parental consent for these age groups may not be in line with GDPR requirements and could disadvantage some students.

3.4.17 All participants registering for a session should acknowledge they have read and understood the code of conduct, which should include the consequences in the case of inappropriate behaviour.

3.4.18 At the start of a session participants should be reminded of this code of conduct, not to take photographs of the screens or share any images, and how they can report any concerns.

3.4.19 If a safeguarding disclosure is made by a participant, the University College's safeguarding policy should be followed.

3.4.20 Staff should not be in a private chat/video call 1-2-1 with a participant. If this happens by accident (someone else loses signal etc.) they should immediately come out of the breakout room/chat/end the session.

Examples of platforms currently in use/being investigated for use by the University include the Neon Online Outreach platform, Brightside, Microsoft Teams and Zoom (for over 16's only).

4 Disclosure and Barring Service Checks (DBS)

DBS checks are required for some people involved in online delivery; the requirements for this are outlined in this policy.

To carry out a DBS check on somebody working with young people in an online space they must meet this criterion:

Individuals who are involved in sessions or monitor the content of internet-based services aimed wholly or mainly for use by under 18's on more than 3 days in a 30 day period. They must also:

- be able to access and remove content or prevent it from being published

- communicate directly with participants aged under 18 years of age
- control who uses the service
- have contact with the children/young people using the service

In these circumstances Health Sciences University will request an enhanced DBS certificate for the person's current role, to be applicable for working with children and young people.

5 Key contact details

For questions, to discuss this policy further or raise a concern, please contact Lisa Bates, Access and Participation Manager by emailing lbates@aecc.ac.uk

Version:	2.0
Approved by:	Senior Management Group
Originator/Author	L.Bates
Policy Owner	Deputy Vice Chancellor
Reference/ source	HE Exemplars
Date approved	8th December 2020
Effective from	9th December 2020
Review date	9th December 2023
Target	All staff and Students conducting/supporting online outreach activties
Policy location	SIP/VLE, Public website
Equality analysis	No direct impact.
Amendment	Minor amendments in December 2020, following advice from The Safeguarding Association. Main changes around parental consent for 16-18 year olds and DBS checks for those working on outreach initiatives.