UNIVERSITY OF CAMBRIDGE
Academic Division
Cambridge Admissions Office

Online Safeguarding Policy
(Version 2: 13 May 2020)

Introduction

This document is designed to provide Cambridge Admissions Office (CAO) staff and other University staff working with CAO 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 Vulnerable Adults. This document was written with specific reference to online activities including, but not limited to, 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 other children/young people.

This policy refers to any and all staff involved in the delivery and supervision of online work. This includes CAO staff members, University or College, as well as temporary workers, such as student ambassadors and residential supervisors.

Risk Assessment
A risk assessment needs to be written which is to be approved by the Line Manager and Head of Team for any new type of activity. The risk assessment will be shared with all members of staff involved with the activity.

Online Platforms
Any online activity should take place on approved online platforms only. These platforms will need to have the following features:

- Access to the platform is enabled only for the intended participants
- Personal information (including names, contact details and email addresses) is only accessible to those with the right permissions and is not publicly viewable
- Staff are able to remove people from the platform if necessary

Examples of currently in-use platforms include the Virtual Open Day and Virtual Tour platform (supported by GoToWebinar) developed by CAO, the Sutton Trust Online platform, MyTutor and Brightside Mentoring. Microsoft Teams and Google Meet are University-supported platforms which may be suitable for some forms of online delivery.

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 monitor the content of internet-based services aimed wholly or mainly for use by children 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*
- *control who uses the service*

- *have contact with the children using the service*

An enhanced DBS certificate will need to be issued by the University of Cambridge, for the person's current role, and applicable for working with children. A member of CAO staff will need to see a copy of the certificate and record the certificate number before staff are given access to any online platform.

Types of Online Activity

Non-Interactive Livestreaming

This section refers to live streaming video or webinars where participant video/audio is not enabled.

The platform must:

- Be appropriate for the participants' age group
- Enable you to restrict the audience to just the intended participants
- Ensure that participants personal information (e.g. contact information) is not visible to anybody else presenting or viewing the stream
- Enable you to reject or force somebody to leave the session if necessary.
- Enable you to control whether participants are able to have their videos/microphones on
- You must make sure that you comply with any safeguarding policies belonging to the platform

Prior to running a live session you should:

- Familiarise yourself with the University's safeguarding policy and the CAO Safeguarding reporting procedures
- Ensure you have the contact details of your Designated Safeguarding Officer on hand and they are aware the session is taking place
- Ensure you have enough staff to support the event. At least two members of staff should be present to supervise the activity. **It is recommended that at least one of these have a DBS check.** We would recommend one member of staff presenting and the other member being present and monitoring any messages on the platform.
- We would also recommend having another member of staff available to call on as a back-up for the event, in case one staff member is unable to attend (e.g. due to illness, connection problems). The back-up staff member does not need to have a DBS.
- Ensure all contributors are employed by the University of Cambridge or one of its Colleges
- Familiarise yourself with the privacy settings and know how to report offensive and abusive content
- Make sure you are using an institutional account (not a personal account)
- Ensure that all staff supervising the activity are familiar with the platform and understand how participants will be using it
- If you are planning to publish a recording of the webinar you should ensure that you have a signed media consent form for anyone identifiable in the recording
- Plan the structure and content of the activity carefully to ensure that discussions remain on topic
- Define a clear time and space for the webinar to take place. (e.g. participants should only be able to contact the speakers/contributors and vice versa during the webinar on the agreed platform)

You should also ensure 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

During the live session:

- 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
- Supervising staff should monitor interactions (verbal and in live chats) to check it is appropriate and relevant, and to deal with any sudden changes or upsetting developments. If delivering or facilitating another member of staff should do this
- 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 re-joining is not possible, then the back-up staff member should be contacted and they should try to join the session as soon as possible to maintain the supervision ratio
- 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
- 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
- If staff share their screens at any point they must ensure that there is nothing inappropriate on the screens/internet pages/browser history
- Challenging behaviour or inappropriate comments should be dealt with immediately, which may involve muting or removing the offender from the platform
- If a participant raises a safeguarding concern, or if a member of staff is concerned about a participant, the procedures outlined in the CAO Safeguarding Procedures should be followed

Interactive Livestreaming

This section refers to live streaming video or webinars where participant video/audio is enabled. For example, this might be the case for small group work sessions or meetings.

All of the above guidance on non-interactive livestreaming applies. However, in addition to this, you should also:

- Ensure that you have consent from parents/guardians of any under-18 participants
- Have a signed Code of Conduct from all participants and which includes the consequences in the case of inappropriate behaviour
- Ensure that participants understand the benefits and risks of online sessions and are clear of the purpose for this particular activity
- Remind participants not to take photographs of the screens or share any images of the online session

Staff should not be in a private chat/video call 1-2-1 with a participant unless this was arranged in advance with manager approval. If this happens by accident (someone else loses signal etc.) the staff member should immediately come out of the breakout room/chat and end the session.

Online Mentoring/Tutoring

This section refers to longer term online engagement with young people in a mentoring or tutoring context.

- All staff (including student ambassadors) working with young people in an online context over an extended period should have a valid DBS check, in line with CAO's DBS policy
- All staff working in this context should receive safeguarding training prior to starting their work supporting students and should be clear on how to report concerns
- Staff and participants must both sign a Code of Conduct prior to starting any online delivery
- Staff and participants must understand that all communication must take place on the designated platform and that they must not share contact information; any communications that happen off-platform must be reported to a member of CAO staff immediately
- CAO staff should regularly monitor interactions which take place and respond to any moderation requests as a matter of priority