University of Warwick

Guidance Note on Online Safeguarding

Introduction

The University of Warwick’s Safeguarding Policy recognises that we have an ethical and moral duty to safeguard children and “Adults at Risk” at any time when they are engaging with our staff, students, volunteers and contractors, in University-led activities, whether on or off of our campus, or through online portals such as Microsoft Teams, Zoom or proprietary teaching platforms such as Brightside Mentoring.

This guidance on the use of online platforms applies to staff, students, contractors and volunteers interacting with anyone aged under 18, or who are an Adults at Risk whether they are current students, prospective students, or otherwise participating in University-led activity. Relevant activities would include tutorials, webinars, virtual tours, and other widening participation, outreach, recruitment and admissions provision, or wellbeing support.

Note: Wellbeing Support Services comprises a team of appropriately trained professionals, who routinely deliver practical, emotional, and psychological support online to Warwick students (some of whom will be under 18/ classed as Adults at Risk). They do so in line with nationally recognised wellbeing standards and in accordance with professional bodies, (where relevant), which override certain aspects of the guidance in this document.

This guidance is aligned with the University’s Safeguarding Policy and has been developed to assist University staff and students to safely use online platforms and to ensure that sources of support are signposted to staff needing to work in unfamiliar ways.

Definitions

Child: Anyone under the age of 18 years.

Adult at Risk: The University bases its definition of an “Adult at Risk” on that used within the Data Protection Act 2018 and defines an “Adult at Risk” as someone over 18 years of age who (i) has needs for care and support; and (ii) is experiencing, or is at risk of, neglect, or physical, mental or emotional harm; and (iii) as a result of those needs is unable to protect themselves against neglect or harm, or the risk of it.

Safeguarding and Online Abuse

The NSPCC provides detailed advice on online abuse in relation to children which can be found here: https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/online-abuse/#what-is

However in brief, children and Adults at Risk may suffer abuse via social media, text messages, and emails or in the course of online chats and other interactive online media. Abuse can take many forms, but includes cyberbullying, emotional abuse, grooming, sexting, sexual abuse and sexual exploitation.

Signs of abuse that may be apparent in the course of online interactions could include unexpected behaviour such as coming across as uncharacteristically distant, upset or angry and the use of language that would be viewed as inappropriate or unexpected for a child of that age.

Assessing and managing risk

A specific Safeguarding Risk Assessment must be written and approved by line-management in relation to any new online activity involving children or Adults at Risk, which is not covered by an existing Safeguarding Risk Assessment.
The Safeguarding Risk Assessment should take into account things such as:

1. Whether the platform being used has a “moderator” with oversight of the online activity or has built-in capability to identifying inappropriate language or images.

2. If the platform used is not moderated or otherwise monitored, will a responsible adult (teacher, parent or carer) also be on-line.

   **Note.** When possible, ALWAYS avoid one-to-one online interaction with anyone you believe may be aged under 18 if no other trusted adult is also involved in the call, if this situation occurs by accident for instance because a participant has lost connection, you are advised to terminate the meeting and reschedule it.

3. Whether the platform being used is approved by the University. Check with IT Services before accepting an invitation to use an unknown online platform hosted by another organisation.

   **Note:** IT Services staff may not have come across the platform before, it is therefore essential that you allow sufficient time for them to research the new platform and answer your question.

**In addition also:**

4. Ensure that all participants understand who is taking part and who will be able to see or hear them.

5. Ensure that all those involved, and any trusted adult also present, are aware of what platform is being used and its constraints and limitations with respect to safeguarding and moderation of content.

6. Ensure that the background environment which may be visible to all participants is appropriate.

   **Note:** Some platforms provide a facility to blur or replace backgrounds.

7. Ensure that appropriate precautions are taken to ensure privacy and confidentiality. If working from home do all that is reasonable possible to ensure that family members cannot view participants or overhear the conversation.

8. Ensure that all pop-ups or notifications of income emails etc are disabled during any activity where your screen is or may be visible to participants.

9. Ensure that no contact details are exchanged during the activity.

10. Ensure that staff and students that engage in online activity receive at least a base-level of safeguarding training as detailed below.

Advice and Guidance is available from:

**Safeguarding Advice:** safeguarding@warwick.ac.uk

**Technical Support:** helpdesk@warwick.ac.uk

**Safeguarding Training**

University staff and students taking part in online activities involving children and / or Adults at Risk should complete the EduCare “Child Protection Fundamentals” module which provides a base-level understanding of safeguarding issues.

The package of modules that the University has licensed from EduCare cover a range of safeguarding activities including “Safeguarding Young People”, “Safeguarding Adults”, and “Safeguarding in Sport”.

Access to these modules can be arranged via safeguarding@warwick.ac.uk.
Online Platforms

All online activities which involve participants that are, or maybe under 18 or Adults at Risk must be hosted on a platform that has been approved for that use by IT Services or a departmental manager with relevant knowledge.

Any such platform must have the following features:

- The ability to restrict access so that only the intended participants may take part.
- Access to sensitive personal information, including contact information (email, mobile phone, social media) are only available to the meeting organiser / host and can be kept confidential.
- The ability for the host to remove anyone who is behaving in an inappropriate manner.

Careful consideration must be given to the suitability of a platform for its intended use. Currently Microsoft Teams and Zoom are both used by the University in appropriate circumstances, however the use of Zoom is not recommended for discussions of a highly sensitive nature where it is necessary to share sensitive personal data. Whichever platform is used, it is important that the most up-to-date version of these platforms are used to ensure that security features are fully implemented and that the meeting host has sufficient knowledge of the platform to be able to enable the controls within the platform’s <Setting> menu to ensure that the above minimum features are enabled.

Some training on understanding how meetings within platforms and recordings work/are shared have been recommended by the IT services team as below:

https://warwick.ac.uk/services/its/servicessupport/academictechnology/research/research-interviews

https://warwick.ac.uk/services/its/365collaborate/microsoftteams/teaching/recordings/

https://warwick.ac.uk/services/its/365collaborate/meetings/teamsguidance/

Note: For complex, large scale events both Teams and Zoom have “special” versions with additional moderating and presentation tools, however it is really important that such large scale events are hosted or co-hosted by someone with relevant experience who is very familiar with the package as this will avoid a lot of problems and potential embarrassment.

The IT training team are happy to discuss any particular requirements meeting organisers may have and can be contacted below:

https://warwick.ac.uk/services/its/servicessupport/training

Additional platforms which are appropriate for some activities include OurWarwick, Meet and Engage, Blackboard Collaborate, the Sutton Trust Online platform, MyTutor and Brightside Mentoring. A number of other organisational also provide similar platforms. When using a third-party organisation (or partner) to engage participants in an online capacity, a review and oversight of their safeguarding policy should be complete prior to the activity and referenced in the risk assessment.

Advice and Guidance:

Microsoft Teams:  
Microsoft Teams

Using Zoom Securely:  Privacy and Security Zoom Communications

DBS

In most circumstances if the guidance in this document is followed, staff and students engaged in online activity involving participants who are under 18 or an Adult at Risk, will not meet eligibility criteria for an Enhanced DBS or an Enhance DBS with Barred List check. However some roles may be eligible for a DBS for instance if the role involves monitoring the content of internet-based services aimed wholly or mainly for use by children on more than 3 days in a 30 day period and the person concerned can:
- access and remove content or prevent it from being published.
- control who uses the service.
- have contact with the children using the service.

Staff in professional roles which involve online wellbeing counselling, mentoring and tutoring of under 18s and Adults at Risk online are likely to meet eligibility criteria for an Enhanced DBS and Barred List Check dependent on the type of advice and guidance provided and the frequency of contact.

Advice and guidance on DBS checks can be found here:
Staff: DBS@warwick.ac.uk
Others: Safeguarding@warwick.ac.uk

Guidance for online events and meetings
In addition to the general guidance provided above on Safeguarding Risk Assessments, Safeguarding Training and Online platforms, also consider the points below when engaging online with participants who are aged under 18 or who are Adults at Risk:

- Where possible / practical always record sessions, but always make it clear to the participants that the session is being recorded.
- Always get parental approval if involving anyone under 16.
- Avoid “live sessions” when at all possible for anyone under 16, (ie use recorded content with no live interaction).
- Do not let participants share screens.
- Do not let participants directly contact any other participant ie all chat goes through the host so that it can be moderated.
- Always have a second member of staff on the session to monitor and moderate the chat boxes
- Use platforms that allow you to disable the participants’ cameras and microphones when this is desirable, for instance if a participant becomes disruptive.
- Use waiting rooms to monitor and control who joins the meeting.
- Set out “community rules” so that participants are aware of the expected behaviour in the online session.

Note: An example of “Community Rules” can be found on the OurWarwick Offer Holders Community pages here: https://our.warwick.ac.uk/community-rules/.

Note: Staff in Wellbeing Support Services should follow appropriate guidance from their Professional Body over arrangements for online professional consultations.

Non-Interactive live streamed events: Participant video/audio is not enabled.

- Ensure the content is appropriate for the participants’ age group.
- Ensure that participants watching the live stream cannot be seen or heard by other participants.
- Ensure participants are aware of how to raise concerns if they should see or hear anything upsetting or inappropriate in the course of the online event.
- Ensure the host department’s safeguarding escalation route is available and that this includes contact details for staff with safeguarding responsibility within the department and the University.
Note: Concerns can also be directly to safeguarding@warwick.ac.uk.

- When using a platform such as the Sutton Trust, MyTutor or Brightside Mentoring, ensure that the meeting host is aware of and can comply with the Safeguarding Policy of the platform being used.

- Always arrange meeting using a Warwick IT Account and if possible use a Warwick licensed platform. Never use a personal email account to set up a meeting or event and where possible avoid using a platform licence which is held in a personal capacity.

  Note: The use of “free” personal licences for platforms such as “Padlet” can lead to difficulties should a safeguarding concern arise, where possible always use a University licensed application.

- Ensure that it is possible to monitor any messages or comments made on the platform’s <Chat board>. It is likely that a second member of staff in addition to the presenter will be needed to facilitate this.

- Ensure that all staff involved in the online session are familiar with the platform used and are authorised to use its control options to prevent inappropriate actions by participants.

- If there is a need to share a screen, ensure that there is nothing inappropriate or confidential on the background of the desktop for instance internet pages, browsing history, emails and pop-ups.

Interactive live streamed events: Participant video/audio is enabled.

In addition to the above:

- Ensure that consent has been obtained from parents/guardians of any under-18 participants and their confirmation that they understand that it would not be appropriate to record the online session, take screenshots, or share images or recordings of the session, via emails or on social media.

  Note: There have been a number of cases where screenshots of meetings shared on social media have inadvertently published the Meeting ID leading to disruption by people from outside the intended audience.

- When inviting participants, be clear on the expected code of behaviour and ensure participants understand that their participation will be terminated and they will be removed from the meeting if they behave inappropriately.

  Note: It is likely that a colleague with “host administrator rights” will need to monitor the meeting so that action can be taken promptly on disruptive or inappropriate behaviour.

- Make use of “Waiting Room” facilities to ensure that only intended participants are able to take part.

- Ensure that the purpose of the meeting is clearly defined and that the discussion remains relevant to the subject of the meeting.

Counselling, Mentoring and Tutoring

Roles held by professional staff within Wellbeing Services are usually subject to an Enhanced DBS and Barred List check. Staff in other roles which involve online advice, mentoring and tutoring of under 18s and Adults at Risk may be eligible for an Enhanced DBS and Barred List check, dependent on the type of advice and guidance provided and the frequency of contact. Relevant roles outside of the University’s Wellbeing Support Service are likely to include:

- Staff and student ambassadors working only or mainly with young people in an online context over an extended period.

- In line with the University’s Safeguarding Policy, staff engaging with under 18s and / or Adults at Risk should complete safeguarding training prior to starting their work. As a minimum this should include a relevant module from the Safeguarding training modules that the University has licensed from EduCare as detailed above.
• In line with the University’s Safeguarding Policy staff engaging with under 18s and / or Adults at Risk should ensure that they are aware of their department’s safeguarding escalation route and know how to report concerns to the University Safeguarding Team via safeguarding@warwick.ac.uk.

• Student Ambassadors should sign a Code of Conduct prior to starting work.  
  **Note:** University staff do not need to sign a code of conduct as they are contractually obliged to follow the University’s policies, safe working practices and guidance on safeguarding.

• All contact between staff and student ambassador with under 18s and Adults at Risk must take place via approved platforms. **There are no circumstances** in which it is acceptable to share personal contact details or make contact with participants through personal social media accounts.

Any member of staff or student ambassador who becomes aware that inappropriate contact is being made with participants via personal email or social media must immediately report this as a Safeguarding concern to their line-manager and via safeguarding@warwick.ac.uk.

**Additional Guidance**

The NSPCC published new guidance on the 18th May on “Online safety during coronavirus” which is available here:  

While this guidance was prepared in response to coronavirus, it has useful information on:

• Online Safeguarding Risks.
• Communicating with children online.
• Online Safety and Social media.
• Remote Teaching.
• Training.