

Centre for Teacher Education
Guidance Note on Online Safeguarding

Introduction

The Centre for Teacher Education Safeguarding Policy recognises that we have an ethical and moral duty to safeguard children and “Adults at Risk” whenever they are engaging with our staff, students, volunteers and contractors, in University-led activities, whether on or off campus, or through online portals.

This guidance on online safeguarding 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 and other widening participation, outreach, recruitment and admissions provision.

This guidance is aligned with the University’s Safeguarding Policy and the University’s Online Safeguarding guidance, and has been developed to assist CTE 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. The Centre for Teacher Education has made significant steps in developing and implementing online teaching. CTE students are all postgraduates who are working towards a professional qualification therefore, amendments have been made to the central university guidance to align with current departmental practice and the nature of the PGCE course.

Definitions

Child: Anyone under the age of 18 years.

Adult at Risk: The University, and CTE, 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 either for a child of that age or for the individual.

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 identify inappropriate language or images.
2. 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:

3. Ensure that all participants understand who is taking part and who will be able to see or hear them.
4. 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.
5. 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.

6. Ensure that appropriate precautions are taken to ensure privacy and confidentiality. If working from home do all that is reasonably possible to ensure that family members cannot view participants or overhear the conversation.
7. 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.
8. Ensure that no contact details are exchanged during the activity.
9. 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

CTE staff 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.

Online Platforms

All online activities which involve participants that are, or may be, 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. 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.

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 potentially Adults at Risk:

- Whilst the university guidance states that all sessions should be recorded, within CTE we have agreed that a sample of sessions will be recorded to provide an opportunity for students who cannot engage in the live sessions to access the content. Sessions will only be recorded with staff consent and it will be made clear to the participants that the session is being recorded.
- Whilst university guidance states that participants should not share their screens, within CTE we have agreed that this can happen providing that participants are advised to ensure that there is nothing inappropriate or confidential on the background of the desktop for instance internet pages, browsing history, emails and pop-ups' prior to sharing screens.
- Do not let participants directly contact any other participant ie all chat goes through the host so that it can be moderated.
- University guidance states that all sessions should be moderated by a second member of staff, within CTE we have agreed that where possible and practical this will be implemented but this will not be appropriate for all sessions.
- Use platforms that allow you to disable the participants' cameras and microphones when this is desirable, for instance if a participant becomes disruptive.
- 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/>.

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

- Ensure the content is appropriate for the participants.
- 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.

- 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.
- Ensure that it is possible to monitor any messages or comments made on the platform's chat facility. 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:

- 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: If possible a colleague with "host administrator rights" will need to monitor the meeting so that action can be taken promptly on disruptive or inappropriate behaviour.

- Where possible 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 engaging with Adults at Risk:

- In line with the University's Safeguarding Policy, staff engaging with 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 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.

Any member of CTE staff 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:

<https://learning.nspcc.org.uk/news/2020/may/online-safety-during-coronavirus#article-top>

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.