University of Exeter

Online Events Guidance V2. March 2024

1. Aim

To set out steps that must be followed when hosting online events with external speakers. The normal risk assessment process applies in addition to this guidance, as set out within the overarching University Speakers and Events Policy (Exeter) and Speakers and Events Process (Cornwall).

2. Scope

This applies to online events such as conferences and other speaker events, whether arranged by University staff or students, and where they are held via online collaborative tools such as Zoom or Teams (not exhaustive). The University has published guidance on using the preferred collaboration tools and security guidance can be found under the heading "online event and meeting security" on the Guidance for Online Events webpage. These resources can be used by staff and students.

3. Out of Scope

Business as usual University Committee or Governance meetings to which external speakers are invited. These meetings are subject to the usual governance arrangements.

4. Key risks associated with online collaboration tools

4.1 The following risks have been identified associated with online events:

- **Event content remains accessible to attendees after the event has ended** – this includes access to the chat files, and documents that were shared, whiteboards created etc. These can be searched under Subject Access or Freedom of Information requests. Everything within the event must be treated as "on the record".
- **Risks associated with files or links shared in meetings** - be aware that links or shared files may be malicious, and ensure that you trust the originator prior to clicking on them.
- **Potential for the normal risk assessment process to be bypassed –** this guidance does not replace the standard speaker risk assessment process, which must be followed as set out within the scope section.

5. Steps to take when setting up an event involving external parties

5.1 **Use a collaborative tool that is supported by the University** – the preferred tool is Teams, as the information security protection is stronger than other tools, providing assurance on security and compliance with the GDPR. However Zoom may be used if Teams is not possible.

5.2 **Confirm with your guests that they can use the tool used to organise the event** – they may need to download software ahead of the day.

5.3 **Disable guest screen sharing, other than by those approved to do so** (those booked to speak). Content that speakers will be sharing should be risk assessed as normal. This limits the risk of an attendee sharing inappropriate and unauthorised material. If general attendees are to have the ability to share their screens as part of the event, this should be robustly risk assessed. How would you manage or control a breach of GDPR or other legislation if this occurred?

5.4 **Require the host to be present to start the event** – check to see if you need to enable an option to prevent guests from joining before the host. This limits the potential for data breaches or the sharing of inappropriate material in an uncontrolled environment.

5.5 **Use the waiting room/lobby if your event should be by invite only** – this enables you to screen and grant access in real time, and is only available if the host joins the meeting first.

5.6 **Remember that meeting chat and shared files will be available to attendees after the event** – ensure that these areas are managed. Attendees will be able to download shared documents, and could screen-shot or copy the chat. These can also be searched after the event if there is an investigation, or a Data Subject or Freedom of Information request.

CHANGE MANAGEMENT

Version	Release Date	Originator	Summary of changes
2	06/03/2024	Tracey Tuffin	Addition of UoE guidance for online events web resources
1	14/09/2020	Tracey Tuffin	First publication approved