

Newcastle University

VIRTUAL RO UNIVERSITY FAIR RISK ASSESSMENT

Title of project or activity	Realising Opportunities (RO) University Fair
Manager / Responsible person	Alexandra Murphy, Head of RO alexandra.murphy@newcastle.ac.uk
School	Realising Opportunities, External Relations, Newcastle University
Date of assessment	13/02/2026
Location of work	The activities, for the purpose of this risk assessment, will all take place on University approved, GDPR compliant software, equipment and servers to ensure the safekeeping and protection of participant's personal information.

1.1: Brief description of project or activity

This risk assessment covers work conducted online by Realising Opportunities (RO) on behalf of all Partner universities to ensure the protection of staff, Student Ambassadors, and programme participants.

Students taking part in RO are in Year 12, or their first year of college, meaning the vast majority will be 16-18 years of age.

The RO University Fair forms an integral part of the Realising Opportunities programme with students engaging with staff and Student Ambassadors from the 9 Partner universities who make up the RO Partnership, former RO students, and representatives from selected employer organisations.

The RO University Fair will take place via vFairs, a virtual events platform provider, on **Thursday 12 March 2026** from 16:00 – 18.00.

2.1: Details of hazards, risks and implemented controls

Hazard 1	Selection and procurement of online platforms
Risks	Platform unable to adequately monitor live (or private) chats, unable to record content, no reporting functionality or being not suitable for GDPR compliance.
Controls	- Appoint a platform provider through a rigorous Newcastle University procurement process. - Ensure the platform undergoes rigorous testing in advance to confirm it is suitable for the intended age range. - The Central Team and vFairs will conduct a testing period, involving staff and guest speakers. - List the events, age ranges and types of delivery functionality that the platform is capable of to safeguard against it being used incorrectly.
Hazard 2	Selecting appropriate staff to work on the event
Risks	- Staff/Student ambassadors conducting sustained private communications with participants without holding a valid DBS check. - Staff/Student ambassadors having had no previous training in safeguarding children online or otherwise.
Controls	- DBS checking required for all staff and ambassadors working on the platform. - Staffing is carefully considered, and recruitment practises are rigorous. - Relevant training is delivered by appropriate and experienced people. - Volunteers from Career Organisations to have limited access to platform functionality.
Hazard 3	Ensuring event, platform & content is appropriate for the age group
Risks	Students under the age of 16 accessing an event where there are opportunities for 1-2-1 conversations.
Controls	- RO is aimed at students aged 16-18 - Forward planning to ensure that all content is tailored to ensure this isn't necessary. - Clearly directing students to tried and tested places in which to ask questions. - RO students invited to join platform on an invitation basis only. - Removal/turning off any one-to-one chat functionality by platform providers.

Hazard 4	Inadequate training for staff and student ambassadors
Risks	- Staff/Student Ambassadors being unaware of reporting procedures. - Staff/Student Ambassadors failing to spot a safeguarding concern.
Controls	- Ensure Student Ambassadors have attended an Online Child Safeguarding training session tailored to the RO University Fair and developed by the DSO. - Link Student Ambassadors to RO University Fair Code of Conduct, to sign and return, to demonstrate understanding and agreement. - Ensure all Partner University staff have completed in-house online child safeguarding training at their institution.
Hazard 5	Inadequate Code of Conduct for participants
Risks	- Participants unaware of rules and regulations for partaking in the online event. - Staff/Student Ambassadors not adhering to Code of Conduct or principles outlined in the Child Protection Policy. - Participants accessing harmful content when participating in online event.
Controls	- Ensure Code of Conduct is developed in line with the Online Child Safeguarding document, platform providers and is tailored to the purpose of each event. - Adapt Code of Conduct where appropriate to suit staff, student ambassadors and participants. - Code of conduct makes clear participants should only access websites as recommended by event organisers.
Hazard 6	Security breach
Risks	- Exposure to harmful content, including but not limited to; - Hate fuelled language - Biased content and extreme opinion, including radicalisation - Sexual/pornographic content - Violent/discriminatory behaviour. - Uninvited individuals access the RO University Fair platform using participants log in information.
Controls	- Ensure the event is adequately staffed to address any issues. - Provide advice and guidance for students to use reputable websites for conducting research. - Ensure that if students are directed to conduct own research, that websites are recommended. - No live webinar sessions will run during the event. - All students attending the event must adhere to a strict Code of Conduct which states participants must not share platform login information.
Hazard 7	Data Breach
Risks	Staff, student ambassador or participants personal information being compromised.
Controls	- Implement the Newcastle University's policy for data breaches, including logging the breach and subsequent actions from thereon in. - Informing and keeping the Data Manager informed. - Assurance and approval of security in place by system provider. - Requesting and providing comprehensive training on any platform used (relation to the lead of the online event along with a Deputy for the purposes on monitoring and regulation) - Password protecting logins. - Staff/Student Ambassadors should always use institutional email address. - University equipment supplied by NUIT should be used where possible to ensure additional levels of security. - Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so. - Keep a record of the decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.
2.2: Additional controls to be implemented	
Controls	This Risk Assessment has been developed with reference to the following iVent policies/documentation: Disaster Recovery Plan; Data security and integrity; Cyber Essentials Certificate.

	A thorough Staff Induction process should be adhered to, to ensure that the member of staff has read and understood all necessary precautions involved with undertaking university business online.
--	---

3.1: Assessor		
Name	Signature	Date
Rena Claire	EClaire	17/02/26
3.2: Manager / Responsible person		
Name	Signature	Date
Alexandra Murphy		17/02/2026