Why has the University decided to use Zoom?
The University is using two on-line platforms, in addition to Moodle, in order to support teaching and learning activities during the lock-down period. These are Microsoft Teams and Zoom video conferencing. The University has selected Zoom because it is easy to use and is capable of handling multiple video connections at the same time, up to 100. Microsoft Teams can have up to 250 participants, but limited to display only four video connections at once (due to be increased to 9 by the end of April). We believe that having the ability for students to see one another and the tutor, is the closest we can get to recreate a normal lecture environment.

Is Zoom safe to use?
Zoom has seen a very rapid growth in its adoption, due to its free version and ease-of-use. It has consequently come under a great deal of scrutiny for some of its security issues, some of which have been featured in the national news media. Due to these concerns, some organisations including the NHS and banks have banned the use of Zoom.

The University of Bolton considered the security issues carefully before buying Zoom. We have decided that Zoom best fits our needs and the identified security issues can be managed adequately, with relevant controls. Most of our teaching and learning content and interactions are not going to be highly confidential, sensitive, or monetarily exploitable to scammers.

As with other software, including Microsoft Office, Zoom are continually updating and closing down security vulnerabilities in their product. It is very much in their interest to do this given the publicity and demand for their product.

What steps are the University taking to ensure Zoom is used safely?

1. The University has purchased the Zoom for Higher Education version of the product. This version integrates with Moodle and provides additional safeguards for students.

2. Teaching staff will set up seminars/lectures on Zoom via Moodle activities. This limits the distribution of the meeting details and the unique password to only the student cohort on the module. Using closed meetings like this mitigates "Zoom bombing", where an impostor can disrupt the Zoom session.

3. Teachers are able to record the Zoom meeting for those students who cannot make the meeting, and for later reference by students. Students are given an option to opt out of the Zoom recording. If a student opts out, they will be dropped from the session, but will be able to view the recording afterwards. The recordings are important for the students who cannot make the session at the scheduled time. Your tutor will be happy to pick up any questions you have afterward following the meeting, if you decided to leave the meeting.

4. All recorded Zoom sessions are password protected to prevent them being viewed by anyone outside the module cohort. The University considers general lecture and seminar content as unlikely to be highly confidential.

Are there cases when Zoom or Teams should not be used for calls?

The University is not recommending the use of Zoom or Teams for confidential meetings such as student counselling sessions. This is not because of any perceived greater risks, but because It is important that both the counsellor and student have absolute confidence in the confidentiality of the call.

The pragmatic alternative for a confidential call is a telephone or the Signal App. Signal is an opensource end-to-end encrypted call App for secure 1-2-1 communication.

Does Zoom hold my personal data?

The University has set up Zoom to use your University email address and your name for your Zoom account. The University does not regard these details as sensitive personal information, and this has been confirmed by the information Commissioners office. You have the ability to change your name in your Zoom profile and also within a meeting if you wish.

Like other service providers, Zoom collects information such as a user's IP address and OS and device details to deliver the service. The Zoom data privacy statement can be found here: https://zoom.us/privacy

The University has set up our Zoom instance to use a European data-centre, and verified that Zoom complies with European general data protection regulations (GDPR).

Can Zoom calls be intercepted?

Zoom does not have true end-to-end encryption like WhatsApp. Instead it has secure, encrypted transmission to and from the Zoom data centres that provides the service. This is the same for most multi-participant conference tools including MS Teams/Cisco WebEx/Google. It means there is part of the call route (in the data centre) where conversations could potentially be intercepted. Zoom have stated that they take steps to ensure the security of calls passing through their data centre

What are the Zoom security weaknesses and how is the University addressing/mitigating each?

Issue	Mitigation
Zoom Bombing	All meetings will be closed and will use a unique password for access. The password will only be accessible to those invited to the meeting. This reduces the risk of intrusion. For students, the Moodle module/course will be the gateway to the session. Participants using the web client will need to authenticate prior to joining meetings. Teachers should enable the waiting room

	function before the meeting starts and admit students one by one, or all at once. This can be enabled in the zoom portal by going to Account Management > Account Settings > Meeting > Waiting Room Teachers can also lock the meeting after it starts by clicking "Manage Participants" at the bottom of the screen and select "Lock Meeting". This prevents further participants joining. Meeting organisers should not use social media to share conference/Zoom meeting links as malicious groups can search social media for these meeting ID/links.
UNC path injection' vulnerability allows remote attackers to steal victims' Windows login credentials	This is a wider Windows vulnerability that requires the victim to click on a rogue URL (web link pasted into a chat conversation by a scammer. Using closed groups should eliminate this risk. Meeting organisers should ensure that private chat is turned off.
Unauthorised access to Recordings	Recordings stored on the Zoom Cloud could be accessible because they have a discernible URL structure. Zoom now password protects recording to mitigate this and the University has set passwords to be mandatory. The password would only be available in Moodle.
No end-to end encryption on calls	This is correct. However, all Zoom sessions are encrypted between the clients and the endpoint (Zoom's Servers). The implication means Zoom could decrypt a session if ordered to by a law enforcement agency. The University anticipates that academic content and activities for teaching and learning using Zoom will be low risk and low confidentiality. The University accepts Zooms Privacy statement as part of its contracted terms with Zoom.
Zoom Compromised Accounts	There is a report of list of compromised Zoom accounts for sale. However, many cyber commentators believe that most of these are constructed list relying on user

	details obtained from hacks of other services, and assuming users have used the same login credentials for their Zoom account. The University has implemented single sign-on using your University account. If you believe your University password has become known to any other individual you are able to change your password in the normal way.
Zoom clients containing Malware (PC and Apple Mac)	There have been reports of an old version of Zoom software containing malware. This version is likely to have come from a non-Zoom third party site. Any up to date Antivirus software would pick up this threat. If you do not have Zoom installed, on first use, Zoom will ask you if you wish to download the client software – this will be the latest version. If you do not wish to install the Zoom software client, you can still run Zoom directly in your browser only. You will need to authenticate prior to joining meetings from a web client
Potential Zoom file sharing vulnerability	Now resolved mid April 2020. However, you are recommended to use other methods for file sharing such as Moodle, Teams, E-mail, etc. You should not share files of personal or confidential data without this being encrypted in the normal way.
The uploading of inappropriate materials by attendees during a Zoom meeting	This can be prevented by visiting your zoom online portal and then going to Account Management > Account Settings > Meeting > File Transfer.
Zoom Cryptographic keys issued by Chinese Servers	The University has configured Zoom Service to not use Chinese data centres but only those covered by the GDPR agreement.