The Bar Council

Videoconferencing software, data protection and confidentiality

Purpose:	To guide all barristers on good practice regarding videoconferencing software, and the data protection and confidentiality issues involved
Scope of application:	All practising barristers
Issued by:	The Information Technology Panel
Originally issued:	April 2020
Last reviewed:	April 2020
Status and effect:	**Please see the notice at end of this document. This is not "guidance" for the purposes of the BSB Handbook I6.4.**

1. There are a number of different commercially available software products, which might be technically capable of being used for remote video hearings, and video conferences. These include: Skype for Business, Microsoft Teams, Zoom, Lifesize, Cisco Webex, Bluejeans and Whereby. Lifesize and Whereby explicitly claim to be GDPR compliant, but the IT Panel has not made its own assessment of whether they are satisfactory. In addition, HMCTS has the JUSTICE video service for the criminal courts and is rolling out CVP (cloud video platform) on an accelerated basis for all jurisdictions.

2. HMCTS has issued updated guidance. It explains that only Skype for Business and CVP are currently supported for video hearings and HMCTS does not currently support the use of other video conferencing applications. HMCTS has expressed concerns about the privacy implications of using some platforms, such as Zoom. However, we are aware that other platforms have been used for hearings (see paragraphs 2.2 – 2.4 of The Remote Access Family Court v4, dated 16 April 2020). The software most often being used for video hearings in Family Courts is Skype for Business and Zoom. It seems that in many cases the remote video hearing

has been set up by the legal representatives of a party as opposed to the court (see paragraphs 2.4 and 5.4).

3. The current HMCTS guidance states that participants in video hearings using Skype for Business do not need Skype for Business to join these videoconferences, however they will need the free Skype meetings app, which is accessible through the link that will be sent by the Court. The presumption in this guidance is that participants join as guests and do not set up the remote hearing.

4. Skype for Business and Microsoft Teams are both Microsoft products. We anticipate that the Microsoft products are as secure as other commonly used Microsoft products, such as Office, but the IT Panel is not in a position to confirm this. The same terms and conditions and privacy policy apply to Microsoft Office products and Skype. You should check that your privacy settings are appropriate – for further help you can view the Bar Council's guidance here.

5. Zoom's videoconferencing software has been publicly criticised in a number of respects, in relation to security and privacy - see here and here, for example.

6. Zoom's position is that they have sufficiently addressed the concerns which have been expressed – see here and here.

7. One of the criticisms made against the Zoom software relates to encryption. Zoom had stated that their software is end-to-end encrypted, but they now accept that "there is a discrepancy between the commonly accepted definition of end-to-end encryption and how we were using it" – see here. The weaknesses in Zoom's encryption system are considered here.

8. One of the steps which Zoom took was to update their privacy policy. The updated privacy policy does address concerns about Zoom's intentions in relation to the protection of personal data. Previously, Zoom had retained the right to use for its own purposes the data which it obtained from videoconferences, which includes all the content of chat text and records of the conferences themselves. However, even their new terms of service and the sign-up process do not make it easy to identify and to understand the terms which apply to EU data controllers. For example, there is an Addendum to the Terms and Conditions, which includes as an annex, an agreement (for which a signature is required) that adds important protections for data subjects. There is no obvious link to this addendum on the sign up page for guests. Although Zoom now states that it acts only as a processor or sub-processor, the standard terms of service may not meet the requirements of GDPR Article 28 (dealing with the terms required to be included in contracts between data controllers and data processors.

9. One of the limitations of Zoom arises when the invitation is sent to an invitee for a Zoom meeting. The first time the Zoom app is used it requires acceptance of Zoom's privacy policy and terms and conditions - there is no option to accept some but not all of these terms and not all terms are apparent. If you have previously signed up to Zoom or previously downloaded the app, then this option does not appear. It is unclear whether the older terms or the newer terms would apply in that case.

10. The Bar Council's IT Panel is not in a position to state whether Zoom is now sufficiently secure and whether it provides sufficient protection for personal data.

Para 5.20.1 of The Remote Access Family Court states:

> *5.20.1 With respect to GDPR and data protection, information supplied by the FLBA clarifies that the Information Commissioners Office is content that Skype for Business, LifeSize and Zoom (provided in respect of Zoom that the host has indicated that they accept the terms and conditions specifically in relation to GDPR which, in reality, they will have to do as they are not able to set up a meeting unless they have ticked the requisite box) are GDPR compliant. The position with respect to Microsoft Teams will need to be clarified. The Information Commissioner's Office has indicated that reasonable allowances are going to be made during this period of national emergency (see here).*

11. The Bar Council's IT Panel was unable to confirm that the ICO is content that Zoom is GDPR compliant. It therefore asked the ICO to indicate whether use of Zoom by the Bar would place a Barrister using Zoom, (i) as a customer, i.e. setting up the conference and (ii) as a user, i.e. if invited to use Zoom by the Court, at risk of investigation or enforcement by the ICO, and if Zoom is complying with UK and/or EU data protection legislation.

The ICO's initial response was as follows:

> *It would be for the controller of the information to ensure that the personal data is being processed securely and in compliance with data protection legislation. At the moment, the Information Commissioner's Office doesn't endorse a specific practice or software and, therefore, we wouldn't be able to say whether Zoom is compliant. If it is possible to contact Zoom directly, they might be able to give you more specific information about how they process personal information and whether data might be shared with third parties.*
>
> *However, if you have concerns that using Zoom might undermine the security*

of personal information and could potentially result in sharing confidential data, we wouldn't recommend you to use the platform.

In a further letter the ICO said this:

Please be advised that the ICO is aware of concerns being raised by various sectors in relation to the use of Zoom. As such, the ICO is in the process of developing its own understanding of this and other similar platforms. This work is contingent on engagement with other regulatory stakeholders and as yet we are not able to confirm our position regarding Zoom and other systems. Whilst the ICO is in the process of confirming its position on these types of platforms, the GDPR also identifies that there is a responsibility for data controllers to implement their own technical and organisational measures to ensure processing is undertaken in accordance with the regulation. This means The Bar Council will need to draw its own conclusions around the nature, scope and context of the processing alongside any considerations of material that the ICO produces.

12. In its second letter the ICO asked for clarification of whether Zoom was being used for proceedings, and this has been provided to the ICO.

13. The ICO's response confirms that it is the data controller who is responsible for ensuring that personal data is being processed securely and in compliance with data protection legislation. For hearings arranged by the court the data controller is likely to be the court, rather than the barristers who have been invited to participate in the hearing as guests. In such cases, the court should be the data controller, and the court should maintain effective control of personal data which is referred to during the hearing. The barrister may not be in a position to decline to participate in the virtual hearing, and the barrister's role will be similar to the barrister's role at a hearing in a physical courtroom. Where a hearing using Zoom is arranged by the court, concerns about barristers' GDPR compliance therefore may not be as significant.

14. There could however be greater concern about GDPR compliance in a case where the hearing using Zoom is arranged not by the court but by one of the parties' legal representatives.

15. Where private chat and break-out rooms are used by barristers as an adjunct to the virtual hearing, the information which is communicated is likely to be considered to be under the control of the barrister, and they may well be the data controller in respect of any data shared with the platform as a result of using those facilities. The risk under the GDPR will depend, of course, on the nature and extent

of the personal data that is being disclosed, but GDPR is not the sole concern; the confidentiality of those discussions also needs to be protected. Accordingly, a barrister should consider very carefully whether the use of those facilities is sufficiently secure.

16. In some cases, the Court has required parties' representatives to record the hearings and subsequently to send them to the Court. If you are in this situation, you should ensure that you take appropriate information security measures to prevent inadvertent loss or disclosure of the recording. If it is being sent on a USB key, it should be encrypted and sent separately to any password. However, USB sticks are not considered ideal as they are potential vectors for the transmission of Covid-19.

17. Where a platform is selected by a barrister for a video conference, rather than for a hearing, they will be the data controller, with all the responsibilities that follow.

18. As a practical matter, it may be the case that there is only a low risk of enforcement action being taken by the ICO as a result of the use of a widely used videoconferencing software product which does not contain adequate safeguards for the protection of personal data. But, in the absence of any confirmation from the ICO in relation to Zoom, the IT Panel is not in a position to offer any reassurance to barristers that there is no risk of ICO enforcement action being taken against them if they use Zoom. The IT Panel is not in a position to confirm the information supplied by the FLBA referred to in para 5.20.1 of The Remote Access Family Court.

19. Given the criticisms of Zoom which have been widely expressed, barristers may consider it prudent, where possible, to use alternative software which has not been the subject of the same degree of criticism as Zoom. Using a provider which is located within the EEA may provide a solution to some of the problems, which have affected companies located outside the EEA, such as Zoom.

20. Barristers who, after assessing the risks, decide to use Zoom may find it helpful to refer to the precautions recommended by the Electric Frontier Foundation. The Family Law Bar Association has also provided guidance (restricted to members of the FLBA). This FLBA guidance is updated from time to time, and those who use this guidance should ensure that they have access to the most recent version.

21. The IT Panel does not endorse or recommend any particular product.

Important Notice

This document has been prepared by the Bar Council to assist barristers on matters of information security. **It is not "guidance" for the purposes of the BSB Handbook**

I6.4, and neither the BSB nor bodies regulating information security nor the Legal Ombudsman is bound by any views or advice expressed in it. It does not comprise - and cannot be relied on as giving - legal advice. It has been prepared in good faith, but neither the Bar Council nor any of the individuals responsible for or involved in its preparation accept any responsibility or liability for anything done in reliance on it. For fuller information as to the status and effect of this document, please refer to the professional practice and ethics section of the Bar Council's website here.