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:	December 2022
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. This Guidance aims to address some of the points to be considered on privacy, data protection and confidentiality, when using video-conferencing technology.

2. Following the challenges which were presented by the COVID-19 pandemic and the significant improvements in video conferencing technologies, many cases now being heard in England and Wales use audio and video conferencing tools so as to proceed effectively. At the start of the pandemic, The Lord Chief Justice gave guidance[1] that the default position was that hearings should be conducted with one, more than one or all participants attending remotely. This position was reiterated in a statement on 5 January 2021[2], which states that "[*f*]*acilitating remote*

[1] https://www.judiciary.uk/announcements/coronavirus-covid-19-message-from-the-lord-chief-justice-to-judges-in-the-civil-and-family-courts/

[2] https://www.judiciary.uk/announcements/message-from-the-lord-chief-justice-latest-covid-19-restrictions/

attendance of all or some of those involved in hearings is the default position in all jurisdictions, whether backed by regulations or not."

3. Despite the removal of lockdown restrictions with courts and tribunals returning to business as normal, it is, effectively, a "new normal" with courts and tribunals embracing the greater use of technology to facilitate remote or hybrid proceedings. being open in-person hearings, it is likely that there will be continuous use of telephone, video and other technology to hold hearings remotely. Initially, new guidance on remote hearings was issued by the courts on an ad-hoc basis. However, steps are now being taken to lead to greater uniformity, for example, the issuing on 14th February, 2022 of a Message from the Lord Chief Justice on Remote attendance by Advocates in the Crown Court.

4. Audio and video hearings are subject to the relevant jurisdictional rules and practice directions. The Protocol Regarding Remote Hearings issued by HMCTS outlined (with reference to CPR PD 51Y and also section 85A of the Courts Act 2003) that, with the exception of proceedings that the court directs to take place privately, to ensure the administration of justice, remote hearings shall remain public to the extent that can be achieved. In consequence, even where remote or hybrid hearings take place, most of these will remain public, approximating so far as possible to an in person hearing in open court. Further, with the Judge's permission, live streaming of hearings may also take place over the internet. It should be noted that recording or transmission of proceedings without the Court's permission would be a criminal offence under section 85B of the 2003 Act and could lead to serious sanctions, including either prosecution or contempt of court proceedings, and a report to the BSB. Legal representatives must understand that they are required to follow court directions in relation to remote or hybrid hearings and should not, by their own actions, undermine the integrity of the court process[3]. Further, they should take care to advise their clients of the same, so that links provided to clients are not distributed more widely, without the Court's approval.

5. The **CCBE Guidance on the use of remote working tools by lawyers and remote court proceedings issued on 27 November 2020**[4] (**CCBE Guidance**) also provides useful guidance on the two inter-related aspects to the use of remote video conferencing tools:

[3] https://www.lawgazette.co.uk/news/city-giant-self-reports-to-sra-after-trial-streamed-live-on-zoom/5105294.article

[4] https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20201127_CCBE-Guidance-on-the-use-of-remote-working-tools-by-lawyers-and-remote-court-proceedings.pdf

(1) Consultations, and meetings by lawyers with their clients and others by remote means, which are private and confidential;

(2) Remote participation in Court hearings, which in most cases are public.

6. A number of different commercially available software products are available which might be technically capable of being used for remote video hearings and video conferences. These include (but are not limited to): CVP, Skype for Business, Microsoft Teams, Zoom, Lifesize, Cisco Webex, Bluejeans and Whereby. The CCBE Guidance is based on a series of research papers examining the terms and conditions of a number of frequently used video conferencing platforms and includes an instructive paper on 'Analysis of videoconferencing tools'[5].

7. Barristers should familiarise themselves with the controls available to them in any platform, including the ability to mute and unmute themselves, to switch on and off their own camera, to refine sound and video settings, and, if required and available, to share documents safely. Some settings will be contained within the conferencing interface. Others, for example camera or auto focus settings, may be found within hardware-specific software settings. If your device or computer offers multiple sources of sound, should know where and how in the software you can specify and switch from a default source to a particular microphone or headset you might intend to use. Always consider making a test call on any platform which you have not installed and used before, or with a known platform when using a new device or for a change from your familiar network connection.

8. Consider the impact of lighting and acoustic effects of the environment from which you connect. Mitigate excess echo from hard surfaces and closed doors (e.g. hang a coat). Adjust the height and distance of any equipment or camera to improve the ease with which you can be seen and understood during the conference.

9. Permission of the Court would always be needed for any party to be included as a participant and no party should attempt to use a separate technology (eg a parallel handsfree telephone call or a separate videocall on another device) to extend any visual or acoustic connection beyond the official parties present on a call, though you may require to use a parallel channel of communication to receive

[5] https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20201127_Annex_Analyses-of-videoconferencing-tools.pdf

instructions from your instructing solicitor during the course of proceedings if you are not in the same location as the solicitor.

10. There are particular issues related to any intention to participate from abroad. Consider Agbabiaka (evidence from abroad; Nare guidance) [2021] UKUT 286 (IAC). This case concerned the procedure to be followed when a party to a case wishes to rely upon oral evidence given by video or telephone by a person (including the party themselves) who is abroad i.e. in the territory of a Nation State other than the United Kingdom. In September 2022 The First Tier Tribunal (Property Chamber) Presidential Guidance Note 1 of 2022 – Giving Evidence from Abroad sets out relevant issues[6].

11. If you are participating in a conference away from Chambers, satisfy yourself before you start that your intended connection method is of adequate speed and quality. Use a speed testing website[7] to check your upload and download speeds. For any new place or network you use, make a test call, preferably on the platform you intend to use, or at least use the HMCTS CVP platform to make a test call to establish the adequacy of any particular network connection for video and voice quality[8].

12. With domestic broadband, internet speeds are typically substantially asymmetric such that information flows into the home much faster than it leaves. Pay particular attention to your upload speed. As a consequence of this asymmetry, there is risk that, on a shared domestic connection, other participants in the conference or call might find your camera picture frozen or sound unintelligible long before you appreciate that there is a problem with your connection. If you are proposing to use a shared connection with an upload speed likely to be on the edge of acceptable video and audio quality (e.g. slower than 2Mbits) consider asking others in the household on the same connection to minimise their use during conferences or hearings. You may want to consider detaching from a Wi-Fi or legacy fixed internet connection and switching to your cellular connection if, on testing, you establish that this gives you an improved uplink connection. Although this may sometimes lead to a slightly reduced maximum download speed, this may not matter as the download speed is likely to be well in excess of what you would need for you to be able to see and hear other participants in a video conference. Do not assume that the Wi-Fi or fixed connection in a building will necessarily give a better overall experience than using a tethered connection

[6] https://www.judiciary.uk/wp-content/uploads/2022/09/Presidential-Guidance-Note-1-of-2022-Giving-Evidence-from-Abroad-FINAL.pdf

[7] For example: https://speedtest.net

[8] https://join.meet.video.justice.gov.uk/HMCTS/#/?conference=test_call

or a mobile device with its own mobile (cellular) internet connection. Consider acquiring an exclusive and dedicated internet connection for your professional use.

13. Different software may operate at a very different quality on different hardware running at the same place and on the same connection. If you have a choice of equipment to use for your Videoconference, if possible, try alternatives on the particular platform before the live hearing. Try unloading or closing unnecessary applications before you start. For example, online backup or photo cloud synchronisation would compete with your limited uplink. Prioritise closing programs that are likely – without warning- to congest or saturate your uplink during the videoconference.

14. HMCTS uses a number of platforms, i.e., BT MeetMe, Cloud Video Platform (CVP) (based on the Kinly platform), but does not require any additional security measures[9] to be taken when using the platforms, beyond using an up-to-date internet web browser. See HMCTS's guidance How to join Cloud Video Platform (CVP) for a video hearing (updated 29 July 2021). You can check your internet browser and test your camera, microphone and speakers by making a test call.
15. HMCTS offers a range of online training. See its September 2020 article Inside HMCTS: Building confidence in using the Cloud Video Platform for hearings[10].

16. The ICO has issued a blog titled 'Video conferencing: what to watch out for', which outlines the key issues which should be considered when using video conferencing technology, including:

    (1) *transparency of video conferencing technology*—providing participants with information on how their personal data will be processed through the privacy and security features of the platform, and how to change any settings.

    (2) *awareness of phishing risks* associated with emails and the chat functions on the platforms, and bringing awareness to participants of the risks of the 'live chat feature', which can be used by cyber criminals to spread phishing messages through links or attachments;

[9] https://www.gov.uk/government/publications/how-to-join-a-cloud-video-platform-cvp-hearing
[10] https://insidehmcts.blog.gov.uk/2020/09/01/building-confidence-in-using-the-cloud-video-platform-for-hearings/

(3) *choice of platform*—the video conferencing platform's privacy policies should be reviewed to ensure its use also conforms to the user's own privacy policy.

For sensitive and private hearings, the need for end-to-end encryption should also be considered.

17. Lifesize and Whereby explicitly claim to be GDPR compliant, but it will be for the data controller to determine whether any platform is suitable and complies with the data controller's own privacy policies. The IT Panel has not made its own assessment of whether they are satisfactory. In addition, HMCTS uses the JUSTICE video service for the criminal courts and is rolling out its CVP (cloud video platform) on an accelerated basis for all practice jurisdictions.

18. HMCTS issued updated guidance in November 2020. This guidance explains that Skype for Business and CVP are currently supported for video hearings. HMCTS has expressed concerns about the privacy implications of using some platforms, such as Zoom. However, since then, the IT Panel has found that Microsoft Teams is most commonly used in the civil jurisdiction (High Court). Other jurisdictions use alternative platforms (see paragraphs 2.2 – 2.4 of The Remote Access Family Court v5[11] (dated 26 June 2020). The software most often being used for video hearings in Family Courts is Skype for Business and Zoom but HMCTS aim is to transfer all remote hearings to CVP. It seems that, in many cases, especially in the lower courts, legal representatives have been asked to set up and record the remote hearing, as opposed to the court (see paragraphs 2.4 and 5.4). The IT Panel does not advise barristers to take on this responsibility where that can be avoided. Taking on such a responsibility would cause difficulties as to the barrister's role as a data controller and places a substantial responsibility on the barrister for the technical suitability and control of the hearing, which should rightfully be borne by the Court.

19. Skype for Business and Microsoft Teams are both Microsoft products. It may be anticipated that the Microsoft products are as secure as other commonly used Microsoft products (such as MS 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 to Skype. Users should check that their own privacy settings are appropriate – for further help you can view the Bar Council's guidance here.

[11] https://www.judiciary.uk/wp-content/uploads/2020/06/The-Remote-Access-Family-Court-Version-5-Final-Version-26.06.2020.pdf

20. 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. Zoom's position is that it has sufficiently addressed the concerns which have been expressed – see here and here.

21. One of the criticisms made against the Zoom software relates to encryption. Zoom had previously stated that its software was end-to-end encrypted, but it now accepts 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. Zoom has now introduced true and to end encryption as noted in its latest updated guidance on End to End encryption in November 2022[12]. It will, however, be noted that the host requires specifically to enable the end to end encryption facility.

22. One of the steps which Zoom took was to update itshttps://zoom.us/privacy privacy policy on a number of occasions[13]. The updated privacy policy does address concerns about Zoom's procedures in relation to the protection of personal data and in its blog Zoom confirms compliance with the GDPR and CCPA. It should be noted that Zoom in its Privacy Notice clearly states it is a data controller. Further, it should be noted that Zoom is based in the United States. As a consequence of the invalidation by the ECJ of the EU/US Privacy Shield in the Schrems 2 case[14] , Zoom now relies on its incorporation into applicable agreements of the EU Commission's Standard Contractual Clauses. following the transition periods specified by the European Commission (i.e., by 27 September 2021 for new contracts and by 27 December 2022 for existing contracts). See Customer FAQs- New Standard Contractual Clauses -Sept 2021 and Zoom's GDPR Compliance Notice.

23. However, the use of standard Contractual Clauses has been criticised as the use of such clauses shifts on to the data controller the responsibility to be satisfied that the laws and practices of the U.S.A are adequate to ensure the protections afforded by the UKGDPR, Indeed, Zoom says in the Notice that "before relying on the SCCs, the data exporter and data importer are now expected to assess whether the laws and practices in the country receiving the data may undermine the level of protection otherwise provided. To support our customers with this assessment, we've prepared a Data Transfer Impact Assessment ("DTIA") May 2022". Considering that it takes the EU Commission, with all of its resources many months to carry out such an assessment, it is unrealistic to expect that a barrister,

[12] https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2EE-encryption-for-meetings

[13] The latest update being 16 September 2022: https://zoom.us/privacy

[14] C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems

acting as a data controller, would have the resources to be able to do this alone, nor is Zoom's own DTIA necessarily to be relied upon as an independent source of advice.

24. This criticism is not restricted to Zoom, but applies equally to other US-based Cloud Providers. In these circumstances, the Bar Council's IT Panel is not in a position to state whether US based platforms in general provide sufficient protection for personal data.

    However, Para 5.20.1 of The Remote Access Family Court Guide states:

    > *5.20.1 With respect to GDPR and data protection, information supplied by the FLBA clarifies that the Information Commissioner's 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).*

25. The Bar Council's IT Panel was unable to confirm that the ICO is content that Zoom is UKGDPR 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[15] 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.*

[15] 7 April 2020

In a further letter[16] 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.*

26. 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.

27. 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 would 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' UKGDPR compliance therefore may not be as significant. HMCTS has a Personal Information Charter which outlines privacy policies for each type of hearing including civil, criminal and family, as well as any related documentation processed by the relevant court or tribunal.

28. The ICO issued Observations in June 2021 following the joint statement on global privacy expectations of video teleconferencing companies[17] and confirmed ongoing engagement[18] in December 2021.

---

[16] 8 April 2020

[17] https://ico.org.uk/media/about-the-ico/documents/4018778/observations-following-statement-global-privacy-202110.pdf

[18] https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2020/12/update-to-the-joint-statement-on-global-privacy-expectations-of-video-teleconferencing-companies/

29. There could, however, be greater concern about UKGDPR compliance in a case where a hearing using Zoom or other US based platform is arranged not by the court but by one of the parties' legal representatives, an arbitrator or a mediator.

30. 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 the barrister 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 UKGDPR will depend, of course, on the nature and extent of the personal data that is being disclosed, but UKGDPR compliance is not the sole concern; the confidentiality of those discussions (which are likely to include confidential and/or privileged content) also needs to be protected. Accordingly, a barrister should consider very carefully whether the use of those facilities is sufficiently secure.

31. 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 computer viruses.

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

33. 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.

34. Although early criticism focussed on Zoom, whose terms, Conditions and Privacy Policies as they stood in March/April 2020 were noted to have concerning deficiencies (though have subsequently been revised as discussed above), as well as being notably insecure as was demonstrated by the publicised "Zoombombing"

incidents, it is possible that other platforms may give rise to similar, though less-publicised concerns. The IT Panel is not in a position to offer any reassurance to barristers that any particular platform does not give rise to similar risks.

35. Given the criticisms of Zoom which have been widely expressed, and the possibility of similar concerns arising in respect of other platforms, barristers may consider it prudent, where possible, to research carefully such criticisms as may have been raised in respect of the use of the particular platform which is being considered, and carefully to consider the terms and conditions and privacy policies of the relevant platform. Where appropriate, consideration should be given to the use of alternative software which has not been the subject of the same degree of criticism, Further, barristers should consider whether it may be appropriate to obtain explicit consent from the users of platforms in circumstances in which the barrister is a data controller. Using a provider located within the EEA may provide a solution to some of the problems which have affected companies located outside the EEA, such as Zoom.

36. 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.

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

38. Another privacy concern in conducting video hearings from participants' homes, is the extent of extraneous video and audio data captured by microphones and cameras as a by-product of the hearing taking place in participants' homes by video: for example, participants' family members (including children) appearing in the background and personal items, such as family photos or documentation, being visible. To circumvent some of these issues, consideration should be given as to whether participants should be able to blur their backgrounds and whether smart speakers should be turned off, in order to create additional privacy when joining a video hearing or conference.

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.