1. Uploading of documents

Documents are often not uploaded onto the case file for each defendant in a multi-handed case. There does not appear to be any system in place to ensure that all documents served by the Crown are available to all defendants. In a multi-handed case, what is supposed to happen is that the CPS creates a case file for each defendant, and a further, joint file naming all joined defendants. It is often not apparent how many case files there are, and which relate to a particular set of proceedings. Searching the case list for the name of your defendant will not always reveal the existence of other, linked case files.

This causes a number of problems in practice:

a. The CPS will typically only upload documents to one of the case files, which is frequently not the joint file, but one of the single defendants' case files. This frequently happens when defendants are charged and added to proceedings at different times.

b. There are frequently different versions of, e.g. Case Summaries on the single files, which can often include or omit vital material of relevance to other defendants. In a case I had recently, I was for D1 in a fourhander. During the trial, the CPS served scientific (DNA) evidence which they believed related solely to D2, uploading it only to D2's case file. I was completely unaware that such evidence (which in fact also impacted D1) existed until prosecution counsel started to read it out in front of the jury! If there is some reason to retain this multiple-file system, I would suggest that there should be a way of linking associated case files so that documents uploaded to one are automatically uploaded to all.

c. The defence solicitors typically only have access to the case for their single defendant, but it is essential that they also have access to any linked or joint file. An invitation to a single defendant's case should also automatically extend to the joint case file. It may be prudent if the individual case files are used solely for such items as correspondence, defence statements, bases of plea, etc. which relate only to that defendant.

d. There is no provision for uploading Unused Material. Clearly there would have to be a way of restricting access to only those entitled to see it, but that should be possible.

e. In all cases, there should be an accurate and up-to-date record of the official PPE (without which, of course, we don't get paid), whether by the rigorous adoption of such a policy by the CPS, or preferably by some automated system. There is a button, "LAA" which allows you to download a PDF called "Legal Aid Agency Report" which attempts to summarise the number of pages in each section, but this is often incorrect, mislabelled and is not, in any event, accepted by the LAA for billing purposes.

DCS is a system that is being managed in an Agile development environment with small incremental updates and bug-fixes being released frequently. We understand the issue of multi-hander cases on the DCS and are currently developing a solution which the Professional Bar have been engaged through invited sessions and workshops as part of the development process.

The summary of the points raised in Question 1 are:-

1 – The process for all cases on the DCS is that HMCTS creates the initial case(s) on DCS and then adds the initial disclosure of the prosecution case (IDPC) material. With multi-hander cases, a lead or 'wrap-around' case is created on DCS where all of the common prosecution disclosure materials are uploaded. Individual 'backing cases' (one per defendant) are also created at the same time for disclosure that should only be shared for that particular defendant (generally PNC at this initial stage). All of the individual DCS cases are linked to the 'wrap-around' lead case. Defence Advocates are each invited to the wrap-around case and their own individual client case.

If defence advocates find that are not invited to two cases per multi-handed defendant case on DCS (per client), then they are to contact the court as the business process has not been followed.

To see what cases are linked to any other case on DCS, simply click on the green "Linked Cases" button on Update Bundle screen.

a. The CPS will typically only upload documents to one of the case files, which is frequently not the joint file, but one of the single defendants' case files. This frequently happens when defendants are charged and added to proceedings at different times.

a. The CPS will upload the common prosecution file to the 'wrap-around' case and any defendant specific material that should not be shared with co-accused to the individually named linked case on DCS. Please see above for the current business process for defence access of multi-hander defendant cases on the DCS.

b. There are frequently different versions of, e.g. Case Summaries on the single files, which can often include or omit vital material of relevance to other defendants. In a case I had recently, I was for D1 in a four-hander. During the trial, the CPS served scientific (DNA) evidence which they believed related solely to D2, uploading it only to D2's case file. I was completely unaware that such evidence (which in fact also impacted D1) existed until prosecution counsel started to read it out in front of the jury! If there is some reason to retain this multiple-file system, I would suggest that there should be a way of linking associated case files so that documents uploaded to one are automatically uploaded to all.

b. This instance is clearly a human error, and a 1-off. We are grateful you have raised this with us and we will issue a reminder to staff of the correct process.

c. The defence solicitors typically only have access to the case for their single defendant, but it is essential that they also have access to any linked or joint file. An invitation to a single defendant's case should also automatically extend to the joint case file. It may be prudent if the individual case files are used solely for such items as correspondence, defence statements, bases of plea, etc. which relate only to that defendant.

c. Yes, agreed. This is the business process, each Solicitor and Advocate should be added to the 'wrap-around' case and the individual defendant case, if this is not happening, they are to contact the court immediately. Under the new multi-hander arrangements being developed on DCS, there will be a single DCS case, defence representatives will only see the common prosecution material and the information pertaining to their client.

d. There is no provision for uploading Unused Material. Clearly there would have to be a way of restricting access to only those entitled to see it, but that should be possible.

d. The CPS are reviewing the use of DCS for Unused Material in "Private Areas" (this is a current facility in DCS), as soon as a decision is made this will communicated widely across CPS Panel Advocates.

e. In all cases, there should be an accurate and up-to-date record of the official PPE (without which, of course, we don't get paid), whether by the rigorous adoption of such a policy by the CPS, or preferably by some automated system. There is a button, "LAA" which allows you to download a PDF called "Legal Aid Agency Report" which attempts to summarise the number of pages in each section, but this is often incorrect, mislabelled and is not, in any event, accepted by the LAA for billing purposes.

e. The LAA Report on DCS was produced in conjunction with the LAA. The LAA Report can only report the "number of pages, and document names" from within the actual DCS case itself, so cannot be wrong. The LAA are working with HMCTS to develop a solution which will allow them access to the cases on DCS.

2. Security Issues

Several issues have been identified in relation to the security/confidentiality of various aspects of the DCS system. I would hope that none of them would maliciously be exploited by a user of the system, but the possibility exists for compromise or abuse.

a. In the case referred to at 1(b) above, in order to gain access to the evidence on D2's case file, the court clerk invited me onto that case (prosecution counsel could also have done this). I was therefore able to access the "Private" Defence Only section and read advices and attendance notes which were presumably not intended for wider consumption.

a. This is a staff training issue and should not of happened (access to the whole of the D2 case on DCS). The individual document should have been downloaded from the D2 case and securely emailed to you **or** added to your clients (D1) individual case on DCS. Again, we are grateful you have raised it and we will address this immediately with staff.

b. Frequently, I have been briefed in a case and have not been invited onto the DCS, or have not been invited onto the main, or joint case, whether through oversight, negligence or whatever. I have found that the best way to get access is to go to the "You are not authorised…" screen and find prosecution counsel, contact them and ask them to invite you on as defence advocate. This ability for prosecution advocates to grant access to defence advocates is therefore useful, but means that merely by designating an invitee as defence that person will then have access to the private defence section. It does not take much imagination to envisage the possibilities for abuse. It gets worse. Prosecution advocates are also able to designate an invitee as a Fee-Paid Judge, which gives that person access to, inter alia, Jury Notes!

b. The DCS business process is that if you are defending, you should be contacting the Court, Instructing Solicitor or Chambers to add you to the DCS case. Prosecution Counsel should not be inviting you to the case as Defence Advocate.

It should be noted that at anytime you feel that there is a possible data breech on the DCS with regards to prosecution/defence access roles, you can immediately highlight this to the DCS Help Desk Email: crimeitsupport@hmcts.gsi.gov.uk

c. I don't know why it was felt necessary to allow users to remove other invitees' access to a case, but you can, and that banned person receives no warning or other notification that this has been done.

d. Similarly, the ability to remove evidence from a case. Why? The fact that the administrators of DCS may be able to examine an audit trail of who did what, and retrospectively uncover any such activity is no justification for permitting these security flaws in the first place.

c & d. Thank you for these interesting points, we will discuss these with the DCS software providers on these issues.

3. Data Protection

I am no expert in Data Protection matters, but it seems to me that our use of the DCS raises all sorts of issues, e.g.

a. As a Data Controller I have to be satisfied that any data I upload to the DCS are being handled securely and within clearly defined parameters. I can't possibly be confident of that, given the matters outlined above.

a. HMCTS are the data controllers for DCS. The ICO's definition of a Data controller is "a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed". HMCTS determine how data is processed on DCS.

The Assurance is derived from the Technical Security risk assessment and IT Health Check (ITCH) carried out on the DCS, which details the Strategic Information Assurance Approach (SIAA) – assurance can be derived from its content.

b. Where does this material go when I upload it? Additional considerations apply to data transferred outside the EEA. Preliminary enquiries suggest that Caselines utilises cloud servers owned by Microsoft and based in the US. As this is outside the EEA, don't I need my client's consent? Even if the data are stored on servers in the EEA, if they are accessed from outside, that is a transfer of data.

b. All DCS data is held within the European Economic Area in-line with Data Protection Act requirements.

c. I have no idea how securely the data are held, for how long it will be retained, what use will be made of it, etc.

c. The security of the DCS is in-line with current Government data security guidelines and signed off by the MoJ Information Assurance and HMCTS SIRO (as defined in the Technical Security risk assessment and IT Health Check (ITCH), Strategic Information Assurance Approach (SIAA). The data is held within the current HMCTS data retention schedule.

4. User Experience

a. The opening of a new tab for each action is annoying, confusing and slows down the browser. There should at least be the ability to alter this in the account settings.

a. This is a user specified setting of how your internet browser software on your device operates. You are at will to change this yourself to your own preferences on how you would like your device and browser to operate.

b. There is no easy way to upload non-document files to a case, e.g. spreadsheets, video clips, etc. The section index down the left shows that a named file is there, but displays a message saying "This document has been recently loaded and the pages are being prepared for display". There IS, in fact, a way to download it, by going to

the "Bundle" section, selecting the relevant individual section and clicking on "Open Original", but that removes the file name and invites you simply to download a file called ".avi", or whatever. There should be a much easier way to upload and access files which are not PDFs or DOCs.

b. The DCS does allow for this, this is the "Placeholder" function, by adding the characters -ph- in the beginning of the file name (lowercase and no spaces), this tells the DCS not to OCR and render into pages within the Evidence Bundle screens in DCS.

At the moment we are not allowing the use of multi-media files with DCS until we can understand the bandwidth requirements of this on the PCU WiFi at court. There is a lot of development work for sharing of multi-media files across the CJS, this is being shared as part of the CJS Common Platform Programme the defence and advocate community are already engaged with.

c. The one single issue which seems to annoy most users most of all is the system relating to Notifications. Could it not be possible simply to alert the relevant people of any change/update by email instead? The current system is indiscriminate, uninformative and time consuming. It appears that the only way to dismiss a notification is to click on the link on the notifications page. The system takes no account of whether the particular update referred to has in fact been viewed, via the main case file, but only through the notification to do so. A number of users (myself included) have experienced difficulties simply viewing notifications at all. Sometimes they are visible and sometimes I simply get an error message without explanation.

c. We are aware of the limitations of the Notifications within DCS and are in discussions with the provider of the system to deliver improvements to this function.