Back up your work: documents, emails and records

Purpose:	To guide all barristers on good practice relating to the backup of material
Scope of application:	All practising barristers
Issued by:	The Information Technology Panel
First issued:	July 2016
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. As a barrister for whom documents are central to your professional function, you will know as a matter of common sense that it is vital to save a backup copy of the work and the electronic files you need to continue working. These may be separate systems which would be useful to you and keep you able to operate professionally in a range of failure scenarios. They will reduce your reliance on any particular system, single device or place. This may be while you're in your room in chambers in order to guard against loss of or damage to your files. Hardware failure, software failure, theft of your PC, or its destruction by fire or flood could all threaten your work and your livelihood. Further risks are the various networks, servers, and power systems beyond your own PC or device which could prevent access to your data for a period which would cause interruption and disruption to your work in Chambers or readiness for Court.

2. A significant threat to your data is deliberate damage by malicious software or data damage or loss caused by others. It may only take one ill-considered click on an attachment to an email or a link in an email, either by you yourself or by one of your colleagues or a member of Chambers staff, for systems to suffer malicious encryption by ransomware. And if this does happen, the ransomware may also encrypt some types of backups, such as synchronised folders on a Chambers server, in a Cloud Storage Service, or on a backup device connected to your PC. Moreover, malicious software can remain hidden for weeks or months before being activated.

3. Consider keeping your data current, synchronised and available in at least three copies of your data, two of which are local and are on different media (e.g., the PC's hard disk drive for your main file storage and a removable device), and one of which is offsite (e.g., a Chambers remote backup or a cloud storage service). These types of storage are discussed below. Remember that if you use a portable media you will have to concern yourself by how data stored on removable media are especially vulnerable to loss or theft and you will have a professional duty to minimize or eradicate impact of potential data theft by using appropriate encryption technologies. You should always consider the physical security of places and storage cupboards in which electronic data devices are held.

4. As you work on a document the electronic file which represents it is likely to be very small- typically measured in kilobytes. You may find that saving regularly the document as a new filename- (File, Save As) perhaps adjusting a suffix on the filename to reflect a document version number, or the time and date of work, provides a ready protection against sudden corruption within the document which would be otherwise be difficult to resolve or for you to reverse changes having saved over the original document. Your intermediate work on the document is then available to go back should there be damage to a table or section which you would otherwise have lost by working constantly over a number of days on a single document or file. Once you are content that a document is finalised- and for example sent back to a solicitor or used in Court, you may then choose to immediately delete many or all your intermediate versions. This small change to your method of working would substantially reduce the chances of total loss of work on that document.

5. What are the most practical ways for you to make effective backups? The following types of backup storage are considered below:

5.1. removable storage, such as a USB memory stick or an external disk drive

5.2. a chambers server

5.3. cloud storage.

Removable storage, such as a USB memory stick or an external disk drive

6. A simple but effective method of making backups is to copy every folder and individual file as you work on them, and again when you complete the work, to a removable stick that connects with a USB port on your PC. Be aware that files can be locked when the word processor program, e.g., Word is open. So close documents or the word processor program before you copy the files.

7. Chose an adequate quality USB drive, giving particular reliance to named storage manufacturers with a USB product that is also listed on their public catalogue or website. The manufacturer should have a known website and supply chain which you should check. Be aware of the large number of USB drives flooding the market through major online channels which are too big to be true for their cost. There are large number of drives which present a much larger size to the computer system than is actually present on the USB. All might go well until you start to save files which in fact start to be written back on top of earlier files which are then corrupted. Run a USB testing utility to confirm the read/write operation on all the advertised data sectors of the device if you are in doubt about the manufacturer or the provenance of the USB device.

8. Unless you have good reason and assured physical security of a physical safe (which could a certified fire safe) and an assured safe physical environment, you should always store professional documents on FIPS140 encryption standard USB drives. The Federal Information Processing Standard Publication 140-2 standard proposed by the US National Institute of Standards and Technology assures the manufacture and the supply chain, as well as the encryption technology are all reliable. This will substantially reduce your professional and information data processing risk profile and show evidence of risk mitigation should the Information Commissioner's Office investigate any data loss should the USB drive be lost or stolen.

9. Consider carefully how much data you store on any single device. In the balance of convenience between having access to all your earlier work and data, and limiting the files you have on a portable USB drive to those of current cases in hand, be cautious to avoid unwittingly carrying thousands of files of data relating to cases you are no longer actively working on. Anticipate the potential loss of a portable device, and actively consider what data you routinely need to be keeping with you as you are travelling between chambers, Court, Solicitors, or your home

office. If you use a device dedicated for periodic backup, and which you keep in a safe, and never carry around, you may form a different view as to what the appropriate encryption technology might be, as necessary, and save a larger number of files on such a device which only travels between your PC and a secure safe close by.

10. You can also back up to a separate larger desktop hard drive, but you should always encrypt this. Encryption software is built in to Windows 10 (BitLocker) and Apple products (FileVault on Mac, Data Protection on iOS and iPadOS), but may need to be turned on. If you use a software based encryption system (such as BitLocker) make a physical record of the decryption key, such that if the drive were used subsequently in a replacement computer or a computer with a reinstalled operating system, you would still be able to gain access. Windows will often store the key used to gain access (encrypt and subsequently decrypt) to a BitLocker encrypted drive without your being particularly aware as a user that there is an encryption key. If you are not aware then without the memory of the key within the particular windows installation or network, you would no longer be able to gain access to the backup drive. So, write any encryption details down and keep that written record physically secret- e.g. printed as a document, within an envelope in a physical safe. Other encryption products are available from other providers.

11. You need to be careful about keeping the device plugged in all the time. While the device is plugged in and active, it is as much at risk of being attacked by malware as the hard disk on your computer.

A chambers server

12. Every well-run set of chambers will have procedures for backing up the chambers electronic diary and fee collection systems. However, it is important to understand that the back-up routines used by the clerks may not include work which has been saved only on a barrister's PC or on the barrister's allocated segment of the network server. Your duties under the UK GDPR as a data processor cannot be transferred to another. So even if Chambers has a backup system, you have a continuing duty to ensure the security, integrity and availability of any data subject to the UK GDPR that you are processing, and so you need to under the basis and details of any chambers system which backup your data.

13. If you believe your computer has been configured so that your files are stored on the chambers network server and that your files may be backed up on a regular basis, you need to understand the specifics of how that process is meant to take place, and how you can check records that such a backup has taken place. As you would not yourself be able to retrieve those backups, and would need to be done by the chambers IT specialist or provider this may take time. You also need to consider the possibility that you will not be able to recover your files if the chambers network is

temporarily unavailable. You should therefore ask for assistance in configuring your computer so that files are saved on your own local computer as well as on the network, for example by understanding or using any Operating System based synchronisation function available in Microsoft Windows logging on to the chambers 'Domain'. If you have installed other cloud backup systems, you need to understand which icons show that those processes are continuing to be effective (i.e., notice a red dot on any taskbar icon) and also, understand how you can see the log of which files have recently been backed up or synchronised.

14. If you or your chambers uses a software utility to synchronise files between a local machine, a server, and perhaps a distant machine, such as a computer in a home office, understand what configuration options are available to synchronise the names of files, and file contents in specific directories. So, for example, you may want a home office, to keep in synchronisation a direction for a case you are currently working on. You are unlikely, given the security arrangements around any home office computer, to want to synchronise all your files to a machine left unattended much or all of the time. Understand the options: and check that for each machine you use, synchronisation continues to operate in the way that you expected when the machine or system was first set up.

15. There is always a risk of malware spreading into a network drive and working its way through file systems and stores systematically. This could occur after a colleague or a member of staff has allowed malware to be introduced, e.g. by clicking on a link in a phishing email. If you use a network store, consider what facilities and permissions are appropriate to secure files not in active use from being changed or deleted. The likelihood is that you will not require routine write access to folders for matters now completed.

16. The main chambers practice management software providers are in the process of introducing sophisticated document management systems which will allow case papers to be stored and backed up in the cloud. These systems are intended to provide robust security, and to facilitate the secure deletion of emails and files which have passed their retention date. The use of these systems should therefore be given serious consideration. Always consider what log systems are in place in relation to file and system access. Plan a method to produce automated regular reports into access, use and changes of files stored on a central or cloud system.

A commercial backup service

17. There are a number of businesses based in the UK or overseas which provide storage in the cloud where you can keep a backup of your work. In some cases, the backup may be made automatically on detecting file changes, or at specified intervals of time. Full or differential backup will transfer all or changed files to the cloud Generally files backed up to the cloud should be encrypted for security. You may have

choices with the provider about whether only you know, or they store the encryption key. Consider setting your own encryption key which the provider does not store. This allows you to reassure the ICO that you have reduced third party risk should there be a data breach on a system for which you have no control.

18. There will be options of reverting back to earlier versions of files on commercial backup systems. Know the options available to you and positively decide what you need. Understand the retention period in any cloud backup service: enquire if your device is not backed up for what length of period would the cloud backup be retained.

19. When you choose a cloud backup service, establish whether or not you can make access to files backed up through any other channel, such as through an online web page or device app. If this is the case, confirm whether a second factor authentication is available to prevent anyone accessing the files in your backup should they predict your username, or anticipate or crack your password. If possible, use an identifier on any backup online system that is not your routine published email address nor easily guessed. Check whether the online backup system is capable of alerting you, by email or app notification, should anyone log on as you, or opt to 'restore' a file. If a notification facility is available turn it on for all notifications.

20. Establish the process to access or restore your files. Some providers include a contractual provision to send you a physical replacement drive should you need bulk access to your file due to system or operating system failure on your PC or chambers system. Restore times – on many backup systems- are considerably slower than backup. Understand how long it would take for you to restore your files. If you do opt for a cloud-based backup system run repeated tests to recover files to establish the full lifecycle functionality of your backup system.

21. Using a cloud based back service may carry risks and disadvantages in relation to security and data protection, which need to be given careful consideration before you sign up to the service. This is particularly but not exclusively the position if you have any criminal practice. The problems include the following:

> 21.1. With some cloud storage services absolute security cannot be guaranteed, particularly if your files are held on a server that is physically overseas or is controlled from overseas. Even if the company providing the service desires to keep your files secure, it may be forced by government, law enforcement agencies, a regulator, or a court, to disclose your files. As already mentioned, these files will almost certainly contain information on other persons which qualifies as 'personal data' under UK data protection legislation. For this reason, all files saved on a remote server (also known as cloud services) should be encrypted by you before being stored – this is known as "end-to-end encryption". With current geopolitical risks of computer hacking and network comprise being elevated, it may be sensible to consider using only a UK-based

cloud-based service for backup.

21.2. Because as a barrister using a PC for drafting you are inevitably processing "personal data" within the meaning of the UK and European data protection legislation, you are required to comply with the General Data Protection Regulation ("GDPR" – see below). If you are sending 'personal data' outside the EEA, even as a backup, you must observe the GDPR restrictions on transferring data to third countries.

21.3. You should not use a server based in any country which is outside the protection of the EU data protection regime, especially if some of your clients are EU citizens. The Safe Harbor regime which formerly enabled the use of US companies' services is no longer available as it does not provide sufficient safeguards for data subjects. A replacement regime – with express contractual terms is being used, but there are serious doubts about whether it provides adequate protection. Some US providers are able to specific UK or EU based geographical storage to address some concerns. Some provide a data impact assessment for you to perform due diligence on any given service.

22. You should also read the details of the terms for any provider very carefully to see what liabilities you may incur to pay the service provider's costs of complying with requirements which may imposed upon the service provider. You should ensure that when your contract ceases you can be sure that the provider will actually delete all your files.

23. You must be careful to make and preserve separately a backup copy of any personal encryption key allotted to you, because if you lose it and have no backup, you are in the same position as if you had lost or destroyed the data.

Organisation of files and emails

24. It is also advisable to adopt a disciplined organisation of your files in folders to make it easy to find and retrieve your work and to enable easy implementation of your data retention policy. Whether you organise your folders by names of instructing solicitors, case names, date, areas of work, or in some other way, the system you devise for your own use needs to be consistent. Because PC search functions tend to be very slow in operation (at least in Windows), it is also advisable to have enough sub-divisions that each folder contains a relatively limited number of files. The reason is that it is easier to retrieve files from a folder that is restricted to a particular case, with sub-folders for pleadings, advice, working notes and so on, than from a folder containing hundreds of files in alphabetical or chronological order. In other words, it is easier to work from hierarchies of folders than from lists of files.

25. Documents relating to anti-money-laundering checks should be kept

separately so that they can be deleted earlier than other documents, and records relating to data protection should be kept together in one place.

26. As mentioned above, new document management facilities included with Chambers practice management software will assist in organising files in a systematic way.

27. Consider arranging access to any cloud based or chambers exchange based email system such that you have consolidated data files in your possession, on a device you control which contain all your emails. Microsoft Outlook (as part of Office 365) along with other programs such as Firefox's Thunderbird synchronises email accounts in cloud services such that emails and their attachments are still available to you in the event that you either temporarily or permanently no longer have working access to the particular email system. Often these programs synchronise the representation of folders, and individual messages within the email system, as a single data file (e.g., an outlook .pst file) or a directory containing individual data files on the PC.

28. You should know how your email client is configured such that you would know which individual file or directory on your computer should be backed up, such that if could be restored and reconnected without reliance on any chambers or cloud system if you needed access in a range of network or system failures.

29. If you arrange to configure your email in this way, be sure that the backup is not achieved through single file synchronisation. If, for example you had a single file representing all the sent emails in 2022, you're yet sending another email would add the data and alter this already very large file. Therefore, some file synchronisation programs would repeatedly attempt synchronisation by repeatedly sending the enormous file over a potentially relatively confined narrow uplink whenever a small part of it was changed by the addition of yet another new email, or even the program marking an unread email as read would trigger the re-upload. If you decide to achieve a business continuity function by ensuring you have file level access to cached files containing emails on your PC, those files will need a periodic and specific backup rather be directories which are configured for inclusion in any automatic or continuous synchronisation process. (e.g.

30. Once you have established a collection of emails stored in a file format which is capable of being read by an ordinary app or software installed on your local machine, you can be confident that you would be able to continue to work with reference to emails already sent and received – with only power to your own machine in the temporary wider absence of electricity or connectivity either to chambers or the wider network.

UK General Data Protection Regulation (UK GDPR)

31. The UK GDPR is the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (EU GDPR) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection Act. Every individual practising barrister is a data controller under the regulations, along with chambers operating through a management company in respect of certain matters. Chambers keeping certain IT facilities for the benefit of members will also fall within the definition of a data processor, and will have to comply with obligations relating to such matters as record-keeping.

32. More information on these obligations is provided in the Bar Council Guide for Barristers and Chambers on the UK GDPR here. You should however also have in mind the UK GDPR's impact on the back-up of data specifically and in light of the points previously set out above.

33. Email and cloud storage providers used to backup data are data processors under UK GDPR. Article 28 requires you to use providers whose terms include obligations
(a) only to process personal data on documented instructions of the controller and
(b) to delete personal data after the end of provision of services. It is not advisable to use services where data is analysed by the service provider's servers (such as Gmail) or mass-market cloud storage which may not comply with this obligation (for example those that are non-EU based).

34. If you are leaving chambers, chambers (as a processor) must, if you request this, either delete or return personal data relating to your cases; but you may want chambers to retain data for a period of time in order to obtain payment of outstanding fees. As part of the process of deleting data, your chambers will need to delete back-up data held by them, and you may therefore wish to have alternative provisions for back-up in place in advance of your departure.

35. Article 17 UK GDPR is also of relevance, as this will enable a data subject to have information held about them erased 'without undue delay' in particular circumstances. This right can't be exercised to the extent that processing is necessary for establishment, exercise or defence of legal claims, or where processing is necessary to comply with a legal obligation of the controller. Should you be subject to an Article 17 request by a litigant or, indeed, any person involved in proceedings on which you hold personal data, these exceptions can be invoked to resist deletion of information which you need to hold for the purposes of defending or taking legal action (for example pursuing a claim for fees or an insurance claim). Thereafter, the data subject's right to deletion will also include the right to deletion of personal data contained in backups. Moreover, Article 25 deals with steps to be taken by data controllers to minimise the amount of data used and stored. Personal data kept in a form permitting

the identification of the data subject must not be kept longer than necessary for the purpose for which the data was processed. The points made in relation to organisation of folders made above may also facilitate the deletion of data by reference to its purpose, e.g., retaining names of clients and matters for conflict checks separate from case papers or work done for clients. Documents relating to anti-money-laundering checks should also be kept separately so that they can be deleted earlier.

Important Notice

This document has been prepared by the Bar Council to assist barristers on matters of IT. **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 see website here.