Back up work on your PC

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:	July 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. If you are a barrister who uses a PC to draft opinions and pleadings, you will know as a matter of common sense that it is vital to save a backup copy of the work, and to do so at a separate location which may be away from chambers in order to guard against loss of your files through theft of your PC, or its destruction by fire or flood or other mishap.

2. Another very serious threat to your data is malicious software. 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 your files to be encrypted 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. For these reasons best practice nowadays is to keep at least three copies of your data, two of which are local and are on different media (eg the PC's hard disk drive for your main file storage and a removable device), and one of which is offsite (eg a Chambers remote backup or a cloud storage service). These types of storage are discussed below.

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

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

4.2. a chambers server

4.3. cloud storage.

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

5. One simple but effective method of making backups is to copy every folder and individual file repeatedly as you work on it, and again when you complete it, to a removable stick that connects with a USB port on your PC. An 8 GB USB stick will generally be sufficient to hold several years' work, and is easily purchased in a computer or stationery shop or online for under £3. It is small enough to carry around in your pocket or bag or on a key-chain. You will also then have all your past work available to you for reference or for a template when working at home, or if you are away from home on a case or a conference. If you also want to back up work-related emails and their attachments you will need a more capacious USB stick, but it is also possible to buy a 64 GB USB stick for under £10. Protect the files on your USB stick with a password and encryption in case you lose it.

6. You can also back up to a separate larger desktop hard drive but you should also 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. Other encryption products are available from other providers.

7. 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

8. 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. It would anyway be risky to rely upon someone else to back up your work. If your computer has been configured so that your files are stored on the chambers network server, your files may be backed up on a regular basis, but you would not yourself be able to retrieve the backups, and this would need to be done by the chambers IT specialist and 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 using the Synchronisation function available in Microsoft Windows.

9. One again there is the risk of malware spreading into a network drive. This could occur after a colleague or a member of staff has allowed malware to be introduced, eg by clicking on a link in a phishing email.

10. 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 much more 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.

A commercial backup service

11. 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 at specified intervals of time. In some cases, your files may be encrypted for security. On the other hand, using such a 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:

11.1. 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 <u>before</u> being stored – this is known as "end-to-end encryption". In the current uncertain political climate, it may be sensible to consider using only a UK-based remote server.

11.2. 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.

11.3. 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 is in place, but there are serious doubts about whether it provides adequate protection. This means US servers are off-limits unless you can be satisfied that the protection put in place meets the standards of protection provided by the Data Protection Act 1998.

12. You should also read the small print 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.

13. 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

14. 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, advices, 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.

15. 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.

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

General Data Protection Regulation (GDPR)

17. From 25 May 2018, the GDPR is directly effective in the UK, increasing the obligations of data controllers set out under the Data Protection Act 1998. 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.

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

19. Email and cloud storage providers used to backup data are data processors under 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).

20. 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.

21. Article 17 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.