How to dispose of your hard drive securely

Purpose: To guide all barristers on good practice relating to the disposal of confidential material

Scope of application: All practising barristers

Issued by: The Information Technology Panel

Last reviewed: May 2017

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.

Need to get rid of your computer? New model? Old one too slow or too heavy? Please read the following advice before you simply sling it in the bin.

Introduction

1. In this day and age, it is likely that all of your data is secured on your chambers’ systems and can be downloaded onto your new computer when you get it. But remember, the chances are that you have copied this data onto your old computer’s hard (storage) drive. Get rid of the computer casually and the data goes with it ready for anyone to get hold of and read. Simple deletion does not do the trick.

2. The Information Commissioner's Office (ICO) has published guidance requiring businesses to ensure that the hard drives of their computers are securely erased before they are sold as second-hand or otherwise disposed of.

3. The Bar Council has, following previous guidance from the ICO relating to encryption, also issued advice on Information Security stating that barristers should ensure they are using encryption software on all their portable or mobile computers, USB drives and removable media (e.g. CD ROMS) used to store documents relating to their practice. This guidance supplements the Information Security guidance.

4. Although further ‘red tape’ issuing from the ICO may be thought to be unwelcome where the risk of misuse of clients' personal information may be perceived to be low, you need to be aware that it is now common for a purchaser of a second-hand computer (e.g. on eBay) to inspect its existing contents. Such inspection may extend to the ‘recycle bin’ for files which have been deleted; and in some cases, enthusiastic purchasers have been known to go to the bother of applying file recovery software in order to find interesting files which have been ‘emptied’ from

1
the recycle bin. Furthermore, the incidence of professional criminals seeking to recover e.g. bank details means that it is no longer safe for a barrister to assume that information relating to his or her cases, which was deleted prior to the disposal of the computer, will never become published on social media or elsewhere. This is so even where the computer is disposed of in an apparently non-working state.

5. An added problem is that USB/Flash drives are often used for a period of time for barristers’ cases, then typically are passed on to others e.g. family members, after which they somehow seem to disappear. New ones are now as cheap as chips, so you simply buy another. We have all done it! Do you know where all your USB memory sticks are? The ‘disappeared’ USB may eventually find its way into the hands of those who would just love to see if there is anything of any interest on it.

6. It is for these reasons that the Bar Council has issued this advice.

7. In general, if you are disposing your device in working order, you should irreversibly delete information on your device using secure deletion software. If you are disposing of your device in non-working order, you should physically destroy your hard drive. If you do not have the technical know-how to do this yourself, you should use a chambers’ IT professional with notice of this advice who can confirm to you that destruction has taken place.

**Physical destruction of devices**

8. Blunt and unsubtle as it may sound, physical destruction is best carried out by removing the hard drive from the computer and hitting it repeatedly with a heavy hammer until the hard drive visibly disintegrates. Your computer’s manual will tell you which screws to undo in order to gain access to the hard drive. Unscrew the hard drive from the interior of the housing and unplug the wires connecting the hard drive to the computer. In the case of very confidential information held on mechanical hard drives, care must be taken to ensure that the rotating disks themselves are shattered. The equivalent for solid state drives is to ensure that each chip inside the device is destroyed individually. However for relatively run of the mill confidential information likely to be held by barristers, provided that the device is destroyed to the extent that it does not function when reinserted into a computer, this is good enough to secure against the type of casual inspection described above.

9. Removable Flash/USB drives which have been used for your cases should be kept securely, should not be given away or lent to family or friends, and if they need to be disposed of, should also be physically destroyed.

**Secure erasure – magnetic hard drives**

10. Secure erasing software is software which writes zeros or random data onto the hard drive, so as to irreversibly ‘cover up’ the existing contents. However, such software cannot usually be guaranteed to work completely where there are already problems with the hard drive of the computer, so should not be relied upon where hard drive errors have been reported by the computer. Examples of such software can be found listed [here](#). For the Apple Mac OSX 10.4+ operating system, Apple provides a utilities called DiskUtility which performs secure disk erasure.

11. Most of these programs are in fact relatively simple to use, requiring you to do no more
than insert a CD-ROM and restart the machine. However take great care when operating the software to ensure that the deletion has been fully carried out before the computer leaves your control.

12. To avoid downloading malware, free erasure applications obtained from the internet must only be downloaded from the primary website, and must be verified by the signing certificate on the primary website before installation, to ensure that they are genuine. If in doubt, use a commercial product.

Secure erasure - solid state drives

13. The software listed above does not work for solid state drives, which make many copies of data all over the device in order to speed up access.

14. Although there are commercial products which purport securely to erase a solid state drive, their efficacy is not known at this time, even where the product is created by the drive’s manufacturer.

15. Hence, in general terms, a solid state drive must be physically destroyed before disposal of the computer – and if the computer is to be disposed of in working order, a new drive will have to be acquired. An exception to this is if the solid state drive is encrypted from new with a long key (password) which is stored separately from the computer, in which case the hard drive may simply be left intact in reliance on the encryption. However this does not mean that it sufficient to encrypt a solid state drive immediately before disposal – the encryption must be present from new.

Secure erasure – iOS devices

16. iOS devices such as iPhones and iPads have solid state drives which are encrypted from new, using a long key which is stored on the device. The devices have a utility for deleting the key: Settings – General – Reset which is believed to be effective to prevent decryption.

17. It is doubtful that such devices will have been authorised for use in cases involving ultra-confidential information of great interest to a hacker, for example terrorism cases, but if they have, then the relevant authorities should be consulted as to how the device should be disposed of – which will probably involve verified physical destruction by the relevant authority.

Secure erasure – other operating systems such as Android

18. Other operating systems such as Android does not encrypt the solid state drive by default. Hence it is up the user to enable this feature. If the feature has been enabled from new, then as for iOS, a factory reset will delete the key and effectively irreversibly erase the contents. If the feature has not been enabled from new, then the device must be physically destroyed after use.

Using a service provider

19. There are a number of companies which offer the services of the secure destruction or safe recycling of computers and devices. However, be aware that some of these companies are less reputable than others, and have been known to provide documents purportedly evidencing destruction or secure erasure prior to resale. Actually, they have not provided the service at all. The
ICO advises you to monitor the service provider, which is rather unrealistic. Nevertheless, ultimately responsibility for the failure by such a company to fulfil its contractual obligation to destroy or securely erase rests with you, as exemplified by a decision of the ICO relating to an NHS Trust.

Summary

20. In summary, the Bar Council’s recommendations are as follows:

a) if your computer is working, and you or a chambers’ IT professional are able to operate secure erasure software, make sure that the software is indeed used correctly to verify that the erasure has completed;

b) physically destroy the hard drive (and any computer device including USBs that may be carrying personal data) yourself, or witness or confirm the destruction of the hard drive by a chambers’ IT professional, to your satisfaction; or

c) if you want to use an external company to recycle electronic equipment, make sure you have a written contract which requires the company physically to destroy the hard drive, to be evidenced with a certificate of destruction, rather than one which permits the resale of the hard drive after alleged secure erasure; do not enter into informal contracts, and do not enter into contracts for free since such contracts depend upon the resale of the hard drive by the recycling company, whereby the risk of personal data leaking out to the public becomes greatest.

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.