



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:	October 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.

Introduction

1. Your computers (e.g. desktops, laptops, tablets, mobile telephones) and removable storage devices (e.g. USB sticks, external hard drives) are likely to contain a great deal of information about you, your clients, and other people concerned in matters on which you are instructed. Some of this will be personal data to which the General Data Protection Regulation (GDPR) applies, and it may include personal data in the Special categories, such as data relating to health, or data relating to criminal convictions. When the time comes for you to upgrade your computer, you need to take precautions to ensure that the data stored on the device is properly destroyed.
2. It is 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 purchasers have been known to apply file recovery software in order to find files which have been 'emptied' from the recycle bin. Furthermore, the incidence of professional criminals seeking to recover e.g. bank details means that it is not safe for a barrister to assume that information relating to his or her cases, which was deleted prior to the disposal of a computer, will never be retrieved. This is so even where the computer is disposed of in an apparently non-working state.
3. The Information Commissioner's Office (ICO) has published [guidance on data security](#). This includes [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.
4. The Bar Council has, following previous guidance from the ICO relating to

encryption, also issued advice on [Information Security](#) and [Mobile Device 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. DVDs/CDs) used to store documents relating to their practice.

5. In general, if you are disposing of your device in working order, you need to irreversibly destroy any information on your device using a method that securely erases the memory. The appropriate method for doing that will depend on the type of device and the type of storage that the device uses. If you are disposing of your device in non-working order, you need to physically destroy the memory. If you are in any doubt as to what steps you need to take, you should take advice from a chambers' IT professional.

Physical destruction of devices

6. 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 (and so will not function when reinserted into a 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.

7. Removable storage such as 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

8. 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 macOS operating system, Apple provides a utility called Disk Utility which performs secure disk erasure.

9. 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

10. The list of software linked to above does not work for solid state drives, which make many copies of data all over the device to speed up access.

11. 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.

12. 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 is sufficient to encrypt a solid state drive immediately before disposal – the encryption must be present from new.

Secure erasure – iOS, iPadOS, and Android devices

13. All modern (since 2015) mobile devices running on iOS, iPadOS and Android are encrypted from new, by default, using a long key stored on the device.

14. Most devices have a utility for deleting the key (for iOS and iPadOS: Settings > General > Transfer or Reset iPhone/iPad; for Android: System > Advanced > Reset Options > Erase All Data) which is believed to be effective to prevent decryption.

Using a service provider

15. There are a number of companies which offer to securely destroy or safely recycle 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 when they have not actually provided the service at all. Nevertheless, ultimately responsibility for the failure by such a company to fulfil its contractual obligation to destroy or securely erase rests with you. The ICO recommends that you check the company's processes first, to be sure that your data will be securely deleted, and that you perform another secure deletion method or at least a 'restore to factory settings' before you send a device off to be destroyed.

16. As a guide, you:

- a. should ensure that 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;
- b. should not enter into informal contracts; and
- c. should 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](#).